(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2003223235 A**

(43) Date of publication of application: **08.08.03**

(51) Int. Cl **G06F 1/00**
G06K 17/00
G06K 19/00
H04L 9/10

(21) Application number: **2002321844**

(22) Date of filing: **05.11.02**

(30) Priority: **26.11.01 JP 2001359940**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

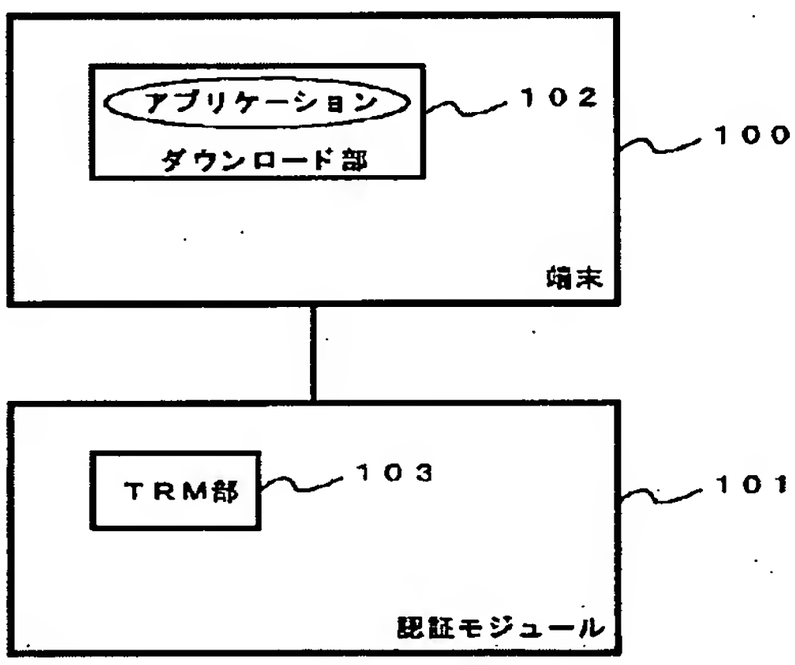
(72) Inventor: **MINEMURA ATSUSHI**

(54) APPLICATION AUTHENTICATION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To solve the problem that the application cannot use local resources of the terminal, since there is a possibility that an operation downloaded to a terminal 100 performs an invalid operation, the operation of the application is rigidly restricted.

SOLUTION: Authentication of the place of origin and whether or not tampering has not been carried out is confirmed, by carrying out authentication of the application downloaded to a downloading part 102 of the terminal 100, using the information for application confirmation retained in an tampering resistant range of an authentication module 101. By only permitting the use of the local resource by the terminal 100 or the authentication module 101 for the authenticated application, the use of the local resource by an invalid application can be prevented. Furthermore, since it is not necessary to provide the tampering-resistant resion to the terminal, manufacturing cost of the terminal can be kept at a low level.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（A）　(11)特許出願公開番号
特開2003－223235
(P2003－223235A)
(43)公開日　平成15年８月８日(2003.8.8)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G06F	1/00		G06K	17/00	L　5B035
G06K	17/00		G06F	9/06	660G　5B058
	19/00		G06K	19/00	Q　5B076
H04L	9/10		H04L	9/00	621Z　5J104

審査請求　未請求　請求項の数42　ＯＬ　（全 43 頁）

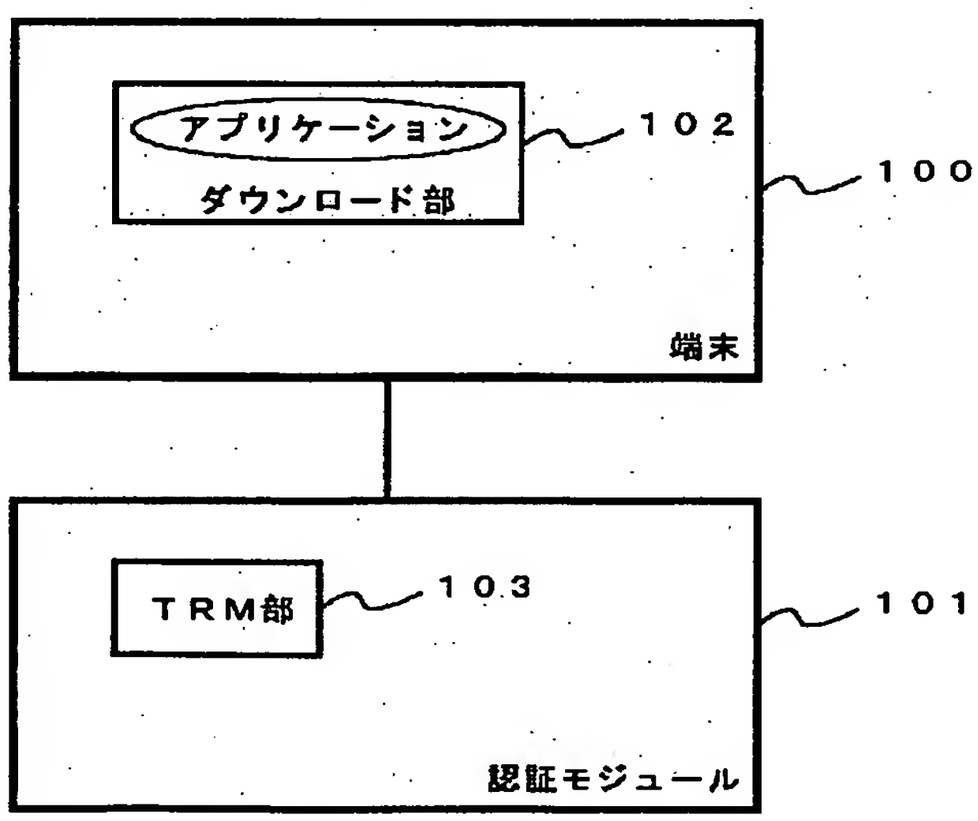
(21)出願番号　特願2002－321844(P2002－321844)
(22)出願日　平成14年11月５日(2002.11.5)
(31)優先権主張番号　特願2001－359940(P2001－359940)
(32)優先日　平成13年11月26日(2001.11.26)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　峰村　淳
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100109553
弁理士　工藤　一郎

最終頁に続く

(54)【発明の名称】　アプリケーション認証システム

(57)【要約】
【課題】　端末１００にダウンロードされたアプリケーションが不正な動作を行なう可能性があるため、ダウンロードされたアプリケーションの動作は、厳格に制限がされており、アプリケーションは、端末のローカルリソースを用いることができない。
【解決手段】　認証モジュール１０１の耐タンパ領域に保持されるアプリケーションの認証のため情報を用いて、端末１００のダウンロード部１０２にダウンロードされたアプリケーションの認証を行い出所の確認や改ざんが行なわれていないかどうかの確認を行なう。認証がされたアプリケーションにのみ端末１００や認証モジュール１０１のローカルリソースの利用を許可することにより、不正なアプリケーションがローカルリソースを利用することを防止できる。また、端末に耐タンパ領域を持たせる必要が無くなるので、端末の製造コストを低く抑えることができる。



【特許請求の範囲】

【請求項１】端末と、認証モジュールと、からなるアプリケーション認証システムであって、
端末は、アプリケーションをダウンロードするダウンロード部を有し、
認証モジュールは、アプリケーションの認証の処理のための情報を耐タンパ領域に保持するＴＲＭ部を有するアプリケーション認証システム。

【請求項２】端末と、認証モジュールと、からなるアプリケーション認証システムであって、
端末は、アプリケーションをダウンロードするダウンロード部と、
認証モジュールに自身が認証されることを条件としてアプリケーションの認証のための処理をするＴＲＭアクセスライブラリ部と、を有し、
認証モジュールは、ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持するＴＲＭ部と、
ＴＲＭアクセスライブラリ部認証情報に基づいて端末のＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、を有するアプリケーション認証システム。

【請求項３】端末の、ダウンロード部は、改ざんのないことを認証するために用いる情報である署名が付加されたアプリケーションをダウンロードし、
ＴＲＭアクセスライブラリ部は、ダウンロード部にダウンロードされたアプリケーションから署名認証用ダイジェストを生成し、
生成した署名認証用ダイジェストと、署名と、を含む署名認証情報を認証モジュールに出力する署名認証情報出力部をさらに有し、
認証モジュールは、署名認証情報出力部から出力された署名認証情報を入力する署名認証情報入力部と、
署名認証情報入力部から入力される署名認証用ダイジェストと、署名と、に基づいて署名の検証を行う署名認証部と、をさらに有する請求項２記載のアプリケーション認証システム。

【請求項４】認証モジュールは、署名認証情報入力部から入力される署名を利用して署名由来ダイジェストを生成するための署名由来ダイジェスト生成情報を取得する署名由来ダイジェスト生成情報取得部と、
署名認証情報入力部から入力された署名と、署名由来ダイジェスト生成情報取得部に保持された署名由来ダイジェスト生成情報と、を利用して署名由来ダイジェストを生成する署名由来ダイジェスト生成部とをさらに有し、
署名認証部は、署名由来ダイジェスト生成部で生成された署名由来ダイジェストと、署名認証情報入力部から入力された署名認証用ダイジェストと、に基づいて認証を行う請求項３に記載のアプリケーション認証システム。

【請求項５】端末は、認証モジュールを認証するための認証モジュール認証部を有する請求項２から４のいずれか一に記載のアプリケーション認証システム。

【請求項６】ＴＲＭアクセスライブラリ部は、認証されたアプリケーションに対して利用を認めるリソースに関する情報であるアプリケーション利用リソース情報を保持するアプリケーション利用リソース情報保持手段を有する請求項５に記載のアプリケーション認証システム。

【請求項７】端末のＴＲＭアクセスライブラリ部は、認証モジュール認証部による認証がされた認証モジュールのＴＲＭ部に対してアプリケーション利用リソース情報を出力するアプリケーション利用リソース情報出力手段をさらに有し、
認証モジュールのＴＲＭ部は、端末のＴＲＭアクセスライブラリ部のアプリケーション利用リソース情報出力手段から出力されたアプリケーション利用リソース情報を耐タンパ領域に書き換え可能に保持する請求項５または６に記載のアプリケーション認証システム。

【請求項８】ＴＲＭアクセスライブラリ部は、アプリケーション利用リソース情報に基づいて、アプリケーションに対して、リソースの利用を認める請求項６または７記載のアプリケーション認証システム。

【請求項９】端末は、署名が付されたアプリケーション利用リソース情報をダウンロードするアプリケーション利用リソース情報ダウンロード部を有し、
ＴＲＭアクセスライブラリ部は、アプリケーション利用リソース情報ダウンロード部にダウンロードされたアプリケーション利用リソース情報に付された署名を検証することを特徴とする請求項６から８に記載のアプリケーション認証システム。

【請求項１０】端末は、署名が付されたアプリケーション利用リソース情報をダウンロードするアプリケーション利用リソース情報ダウンロード部を有し、
ＴＲＭアクセスライブラリ部は、アプリケーション利用リソース情報ダウンロード部にダウンロードされたアプリケーション利用リソース情報から署名認証用ダイジェストを生成し、
生成した署名認証用ダイジェストと、署名と、を含む署名認証情報を認証モジュールに出力するアプリケーション利用リソース情報署名認証情報出力部を有し、
認証モジュールは、アプリケーション利用リソース情報署名認証情報出力部から出力された署名認証情報を入力するアプリケーション利用リソース情報署名認証情報入力部と、
アプリケーション利用リソース情報署名認証情報入力部から入力される署名認証用ダイジェストと、署名と、に基づいて署名の検証を行なうアプリケーション利用リソース情報署名認証部と、をさらに有する請求項６から８に記載のアプリケーション認証システム。

【請求項１１】ＴＲＭアクセスライブラリ部認証情報が、端末に固有の情報である請求項２記載のアプリケー

ション認証システム。

【請求項１２】ＴRMアクセスライブラリ部認証情報が、端末にインストールされているアプリケーションの組み合わせに関する情報である請求項２記載のアプリケーション認証システム。

【請求項１３】ＴＲＭアクセスライブラリ部認証情報が、ＴＲＭアクセスライブラリ部を識別するための情報であるライブラリ識別情報である請求項２記載のアプリケーション認証システム。

【請求項１４】端末は、認証モジュールのＴＲＭ部にアクセスをする端末アプリケーションを保持する端末アプリケーション保持部を有し、

認証モジュールのＴＲＭ部は、耐タンパ領域に、認証モジュール内にて動作する認証モジュール内アプリケーションを保持する認証モジュール内アプリケーション保持部を有し、

認証モジュール内アプリケーションは、ＴＲＭアクセスライブラリ部認証部によるＴＲＭアクセスライブラリ部の認証の成功を条件として端末アプリケーションからのアクセスを受け入れて動作する請求項２から４のいずれか一に記載のアプリケーション認証システム。

【請求項１５】認証モジュールのＴＲＭ部は、ＴＲＭアクセスライブラリ部認証部によるＴＲＭアクセスライブラリ部の認証の成功を条件として認証結果識別子を生成する認証結果識別子生成手段を有し、

認証モジュール内アプリケーションは、認証を示す認証結果識別子の存在を条件として端末アプリケーションに対して認証モジュール内アプリケーションに対するアクセスを可能とし、認証モジュール内アプリケーションは端末アプリケーションからのアクセスを受け入れる請求項１４に記載のアプリケーション認証システム。

【請求項１６】認証モジュールのＴＲＭ部は、ＴＲＭアクセスライブラリ部によるアプリケーションの認証の成功を条件としてアプリ認証結果識別子を生成するアプリ認証結果識別子生成手段を有し、

認証モジュール内アプリケーションは、認証の成功を示すアプリ認証結果識別子の存在を条件として端末アプリケーションに対して認証モジュール内アプリケーションに対するアクセスを可能とし、認証モジュール内アプリケーションは端末アプリケーションからのアクセスを受け入れる請求項１４に記載のアプリケーション認証システム。

【請求項１７】端末と、認証モジュールと、アプリケーションを端末にダウンロードするサーバと、からなるアプリケーション認証システムであって、

端末は、アプリケーションをダウンロードするダウンロード部を有し、

認証モジュールは、アプリケーションの認証の処理のための情報を耐タンパ領域に保持するＴＲＭ部を有し、

サーバは、端末を介した認証モジュールの認証が成功することを条件に端末の認証が成功したと判断する端末認証部を有するアプリケーション認証システム。

【請求項１８】端末と、認証モジュールと、アプリケーションを端末にダウンロードするサーバと、からなるアプリケーション認証システムであって、

端末は、アプリケーションをダウンロードするダウンロード部と、認証モジュールに自身が認証されることを条件としてアプリケーションの認証

のための処理をするＴＲＭアクセスライブラリ部と、を有し、

認証モジュールは、ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持するＴＲＭ部と、

ＴＲＭアクセスライブラリ部認証情報に基づいて端末のＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、を有し、

サーバは、端末のＴＲＭアクセスライブラリ部を介する認証モジュールのＴＲＭ部の認証が成功することを条件としてＴＲＭアクセスライブラリ部の認証が成功したと判断するサーバＴＲＭアクセスライブラリ部認証部を有するアプリケーション認証システム。

【請求項１９】端末と、認証モジュールと、アプリケーションを端末にダウンロードするサーバと、からなるアプリケーション認証システムであって、

端末は、アプリケーションをダウンロードするダウンロード部と、

アプリケーションから署名用ダイジェストを生成する署名用ダイジェスト生成手段と、

アプリケーションのダウンロードと共にダウンロードされた署名を取得するダウンロードアプリケーション署名取得手段と、

取得した署名と、署名用ダイジェスト生成手段によって生成された署名用ダイジェストと、をサーバに送信するアプリ認証データ出力手段を備えるＴＲＭアクセスライブラリ部と、を有し、

認証モジュールは、ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持するＴＲＭ部と、

ＴＲＭアクセスライブラリ部認証情報に基づいて端末のＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、を有し、

サーバは、端末のＴＲＭアクセスライブラリ部を介する認証モジュールのＴＲＭ部の認証が成功することを条件としてＴＲＭアクセスライブラリ部の認証が成功したと判断するサーバＴＲＭアクセスライブラリ部認証部と、

サーバＴＲＭアクセスライブラリ部認証部により認証が成功したと判断されたＴＲＭアクセスライブラリ部のアプリ認証データ出力手段から出力された署名用ダイジェストと、署名と、を入力するアプリ認証データ入力部と、

アプリ認証データ入力部に入力された署名用ダイジェストと、署名と、に基づいてアプリケーションの認証を行なうサーバアプリ認証部を有する、アプリケーション認証システム。

【請求項２０】端末と、認証モジュールと、アプリケーションを端末にダウンロードするサーバと、からなるアプリケーション認証システムであって、

端末は、アプリケーションをダウンロードするダウンロード部と、

アプリケーションの認証の成功を示す認証成功情報を生成する認証成功情報生成手段と、

認証成功情報生成手段にて生成された認証成功情報を出力する認証成功情報出力手段と、を備えるＴＲＭアクセスライブラリ部を有し、

認証モジュールは、ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持するＴＲＭ部と、ＴＲＭアクセスライブラリ部認証情報に基づいて端末のＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、を有し、

サーバは、端末のＴＲＭアクセスライブラリ部を介する認証モジュールのＴＲＭ部の認証が成功することを条件としてＴＲＭアクセスライブラリ部の認証が成功したと判断するサーバＴＲＭアクセスライブラリ部認証部と、

サーバＴＲＭアクセスライブラリ部認証部により認証が成功したと判断されたＴＲＭアクセスライブラリ部の認証成功情報出力手段から出力された認証成功情報を入力する認証成功情報入力部と、

認証成功情報入力部に入力された認証成功情報に基づいてアプリケーションの認証を行なうサーバアプリ認証部と、を有するアプリケーション認証システム。

【請求項２１】アプリケーション本体と、アプリケーション定義ファイルとからなるアプリケーションプログラムであって、

アプリケーション定義ファイルは、アプリケーション本体の属性を示す情報である属性情報格納部にアプリケーションの作成者が自由に利用できるオプショナル領域を有し、このオプショナル領域にアプリケーション本体の署名データを格納し、

オプショナル領域から署名データを取得するステップと、

取得した署名データを利用して、署名を検証するステップと、をコンピュータに実行させるためのアプリケーションプログラム。

【請求項２２】アプリケーションプログラムは、ｉアプリであり、オプショナル領域はＡｐｐＰａｒａｍである請求項２１に記載のアプリケーションプログラム。

【請求項２３】アプリケーションプログラムのデータ構造であって、

コード及びデータの圧縮ファイルであるＪＡＲファイルを格納するＪＡＲファイル部と、

アプリケーションの定義ファイルであるＡＤＦファイルを格納するＡＤＦファイル部と、

からなり、

ＡＤＦファイルには、メインクラスの起動パラメータを格納するＡｐｐＰａｒａｍがあり、

ＡｐｐＰａｒａｍ中に、ＪＡＲファイルの署名が格納されているアプリケーションプログラムのデータ構造。

【請求項２４】ＪＡＲファイルの署名は、アプリケーションプログラムの動作を保証する者による署名である請求項２３に記載のデータ構造。

【請求項２５】請求項２３または請求項２４に記載のデータ構造により、アプリケーションプログラムをコンピュータ読み取り可能に記録した記録媒体。

【請求項２６】ダウンロード部は、ダウンロードアプリケーションのアプリケーション利用リソース情報を記述した署名つきの使用許諾書をダウンロードする請求項２から４に記載のアプリケーション認証システム。

【請求項２７】前記アプリケーション利用リソース情報は、ローカルリソースの種類である請求項２６に記載のアプリケーション認証システム。

【請求項２８】前記アプリケーション利用リソース情報は、ローカルリソースの使用を認める範囲である請求項２６に記載のアプリケーション認証システム。

【請求項２９】ＴＲＭアクセスライブラリ部は、アプリケーションの認証のための処理を、アプリケーションが認証モジュールのＴＲＭ部の耐タンパ領域へアクセスしたことを条件に行なう請求項１８記載のアプリケーション認証システム。

【請求項３０】ＴＲＭアクセスライブラリ部は、アプリケーションの認証のための処理を、アプリケーションがダウンロード部にダウンロードされたことを条件に行なう請求項１８記載のアプリケーション認証システム。

【請求項３１】ＴＲＭアクセスライブラリ部は、アプリケーション認証のための処理を、アプリケーションの実行の開始をトリガとして行なう請求項１８記載のアプリケーション認証システム。

【請求項３２】使用許諾書のアプリケーション利用リソース情報には、アプリケーションが、リソースをアクセスすることができる時間的限度を示す期限日情報が含まれており、

前記期限日情報に基づいて認められる時間的限度がすでに期限切れである場合には、ダウンロード部は使用許諾書をダウンロードする請求項２６に記載のアプリケーション認証システム。

【請求項３３】ダウンロード部は、ダウンロードされたアプリケーションの実行時、又は／及び、アプリケーションの認証時に、サーバより使用許諾書をダウンロードする請求項２から４に記載のアプリケーション認証システム。

【請求項３４】ダウンロード部は、ダウンロードされたアプリケーションの実行時、又は／及び、アプリケーションの認証時に、ダウンロードされた使用許諾書の有効性をサーバに問い合わせる請求項２６に記載のアプリケーション認証システム。

【請求項３５】請求項１ないし請求項２１、請求項２６ないし請求項３４のいずれか一に記載の端末。

【請求項３６】請求項１ないし請求項２１のいずれか一に記載の認証モジュール。

【請求項３７】アプリケーションをダウンロードするダウンロード部と、アプリケーションの認証の処理のための情報を耐タンパ領域に保持するＴＲＭ部と、
を有する端末。

【請求項３８】耐タンパ領域に情報を保持しその情報を用いて認証のための処理を行なう認証モジュールを備えた端末であって、
アプリケーションをダウンロードするダウンロード部と、
認証モジュールに自身が認証されることを条件としてアプリケーションの認証のための処理をするＴＲＭアクセスライブラリ部と、を有し、
前記認証モジュールは、
前記ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を前記耐タンパ領域に保持するＴＲＭ部と、
ＴＲＭアクセスライブラリ部認証情報に基づいて前記ＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、
を有する端末。

【請求項３９】第一の機器と、認証モジュールと、からなるアプリケーション認証システムであって、
第一の機器は、アプリケーションを格納するアプリケーション格納部を有し、
認証モジュールは、アプリケーションの認証の処理のための情報を耐タンパ領域に保持するＴＲＭ部を有するアプリケーション認証システム。

【請求項４０】第一の機器と、認証モジュールと、からなるアプリケーション認証システムであって、
第一の機器は、
アプリケーションを格納するアプリケーション格納部と、
認証モジュールに自身が認証されることを条件としてアプリケーションの認証のための処理をするＴＲＭアクセスライブラリ部と、
を有し、
認証モジュールは、
ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持するＴＲＭ部と、
ＴＲＭアクセスライブラリ部認証情報に基づいて第一の機器のＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、を有するアプリケーション認証システム。

【請求項４１】第１の機器から第（Ｎ＋１）の機器までを直列に接続して出来る（Ｎ＋１）個の機器により構成されるアプリケーション認証システムであって、
第１の機器は、
第２の機器を認証するための情報である認証情報を耐タンパ領域に保持するＴＲＭ部と、
前記認証情報に基づいて第２の機器を認証する第１認証処理部と、
を有し、
第２の機器から第Ｎの機器までのいずれか一の機器を第ｉの機器とする時、
前記第ｉの機器は、
第ｉ認証処理部を有し、
第ｉ認証処理部は、第（ｉ－１）認証処理部に自身が認証されることを条件として第（ｉ＋１）の機器を認証し、
第（Ｎ＋１）の機器は、
アプリケーションを格納するアプリケーション格納部と、
第Ｎ認証処理部に自身が認証されることを条件として前記アプリケーションの認証のための処理をする第（Ｎ＋１）認証処理部と、
を有することを特徴とするアプリケーション認証システム。

【請求項４２】前記第ｉの機器は、第（ｉ＋１）の機器を認証するための認証情報を取得する第ｉ認証情報取得部を有し、
前記第ｉ認証情報取得部は、第ｉの機器が認証情報を格納している領域である認証情報格納領域を有している場合には、その認証情報格納領域から前記認証情報を取得し、第１の機器のＴＲＭ部に前記認証情報が格納されている場合には、第２の機器から第（ｉ－１）の機器までの機器を介して、ＴＲＭ部から前記認証情報を取得する、
ことを特徴とする請求項４１に記載のアプリケーション認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯電話などの端末とＩＣカードなどの認証モジュールとを有するシステムにおいて、端末と端末で動作するアプリケーションとを認証モジュールによって認証する技術に関する。

【０００２】

【従来の技術】従来、ＩＣカードを端末に装着してサーバと商取引操作を行なうシステムにおいては、端末に耐タンパ性を持った領域を確保できないので、サーバ内で動作するアプリケーションプログラム（以下、「アプリ

ケーション」と略す）が直接ＩＣカードを認証するようになっていた。従って、端末は、サーバとＩＣカードの間の通信を中継するのみであった。

【０００３】一方、近年において、携帯電話などにサーバよりアプリケーションがダウンロードでき、携帯端末において動作することが可能となった。

【０００４】

【発明が解決しようとする課題】しかしながら、携帯電話などにダウンロードされたアプリケーションが不正な動作を行なう可能性があるため、ダウンロードされたアプリケーションの動作は、厳格に制限がされている。

【０００５】例えば、携帯電話にダウンロードされたアプリケーションは、携帯電話に装着されたＩＣカードにデータを書き込むことができなかったり、各種インターフェースの使用が制限（禁止）されたりなど、ローカルリソースの使用制限が大きい。

【０００６】また、携帯電話にダウンロードされたアプリケーションは、携帯電話やＩＣカードなどが保持している電話帳やアドレス帳などに記録されたメールアドレスやメールの受信箱に格納されたメールの内容など、個人に関する情報などの読み書きができないように制限を受けている。これは、当該アプリケーションが正規のものであり、携帯電話やＩＣカードなどの内部に保持されている情報にアクセスする権利があるかどうか、また、不正な動作をしないかどうか、という検証ができないからである。

【０００７】このことは、将来的に希望されている携帯ツールの用途汎用化（多様化）やＥ－コーマス（ＥＣ）への応用には極めて大きな阻害要因となる。

【０００８】このような制限を無くするためには、ダウンロードされたアプリケーションを認証してアプリケーションの素性を確認する必要がある。例えば、アプリケーションに第三者が付した署名をアプリケーションとともにダウンロードし、その署名と署名が正しいと検証するのに必要な情報をＩＣカードに提示して認証を行なうことが考えられる。しかし、携帯電話がアプリケーションと署名とをダウンロードした後に、その携帯電話により署名が正しいと判断するのに必要な情報（例えば、ハッシュ関数により生成されるダイジェスト）が生成されるため、ダウンロードされたアプリケーションに付された署名とは別のダミーな署名とその署名により検証ができるような操作が施されたダイジェストが携帯電話によりＩＣカードに提示されてしまう可能性がある。このため、ＩＣカードに提示された署名とダイジェストとが、実際にダウンロードされたアプリケーションのものであるとＩＣカードが信頼することができず、ダウンロードされたアプリケーションをＩＣカードが認証を行なうことができないという問題がある。

【０００９】また、携帯電話などの端末にダウンロードされたアプリケーション（以下、「端末アプリケーション」と略す）がＩＣカードにアクセスできるようにして、そのＩＣカードに保護されるように格納されている情報を読み書きできるためには、同様に、ＩＣカードへアクセスを行なう端末アプリケーションの認証のための処理を、そのＩＣカードが行い、アクセスを許可しても良いかどうかを判断することが必要である。

【００１０】ＩＣカードなどのセキュアデバイスが、それにアクセスを行なう端末アプリケーションを認証するための処理としては、従来は、セキュアデバイスが、そこに保持されているのと同様の秘密な情報を端末アプリケーションが持っているかどうかを判断する、という処理が行なわれていた。しかし、端末には、耐タンパ性を持った領域などの秘密な情報を安全に保持するための領域も機能もない。このため、このような秘密な情報が漏洩する可能性があり、従来の方法では、漏洩してしまった情報を端末アプリケーションが使用している可能性が排除できず、セキュアデバイスが端末アプリケーションを厳密には認証することができない、という課題がある。

【００１１】

【課題を解決するための手段】この問題を解決するために本発明においては、ＩＣカードなどの認証モジュール内の耐タンパ領域に、携帯電話などの端末のＲＯＭに書き込まれたプログラム（以降において、「ライブラリ」と書く場合がある）を認証するための情報を持たせ、認証モジュールは、端末のＲＯＭやＴＲＭなどの容易に書き換えができない領域（以下、ＲＯＭと略する）に書き込まれたライブラリの認証を行なうようにした。

【００１２】このように認証されたライブラリが、ダウンロードされたアプリケーションの署名と共に署名が正しいと判断するのに必要な情報を自ら生成してＩＣカードに提示すれば、ＩＣカードにとっては、認証したライブラリにより提示された署名と情報が、実際にダウンロードされたアプリケーションのものであると信頼することができるようになり、端末にダウンロードされたアプリケーションをＩＣカードが認証できるようになる。結果として、認証されたアプリケーションがＩＣカードにデータを書き込むことなどが可能となり、従来の端末を用いた商取引の操作よりも複雑な操作が実現できるようになる。

【００１３】また、このように、端末にダウンロードされたアプリケーションがＩＣカードにより認証されるようになることにより、ダウンロードされたアプリケーションに、端末の外部インターフェースの利用を許可することも可能となる。

【００１４】また、本発明の実施には、ダウンロードされるアプリケーションの署名をダウンロードすることが必要である。そのために、アプリケーションの署名をアプリケーションとは別にダウンロードするのみならず、既存のデータ仕様にも対応できるように、アプリケーシ

ョンの定義ファイルに格納することを可能とする。このため、署名をアプリケーションのダウンロードとは別にダウンロードすることが不要となる。

【００１５】

【発明の実施の形態】本発明は、端末と認証モジュールとを含むアプリケーション認証システムに関するが、「端末」とは、携帯電話に代表される携帯可能な電子機器であってもよい。また、パーソナルコンピュータや街角に設置させる公衆端末のように携帯が事実上出来ないようなものであってもよく、次に説明する認証モジュールが装着可能な電子機器であり、内部でアプリケーションを動作することが可能なものである。以下に説明するように端末は、その内部に種々なる部を有するが、端末にＲＯＭ、ＲＡＭ、ＣＰＵを備えることにより、このような部は、ソフトウェアにより実現可能となる。

【００１６】「認証モジュール」とは、内部に記憶領域を持ったものであり、（ＳＤ）メモリカード、ＩＣカード、スマートカードがあり、装着された端末からデータを入力するとそれに対する返答を返すという動作を行なう。また、認証モジュールは、耐タンパ領域と言って、そこに格納された情報の不正な読み出しおよび不正な書き換えを防止する領域がある。以下で説明する認証モジュール内の部のいくつかは、このようなＩＣカード内で動作するカードアプリケーションによって実現することもできる。

【００１７】通常、端末に認証モジュールが装着され、端末と認証モジュールの間で電気回路が形成され、情報の交換が行なわれる。ただし、端末の本体と認証モジュールが装着される部分とが分離し、通信によって情報の交換が行われる形態もある。

【００１８】なお、端末で動作するアプリケーションは、算術演算、ローカルインターフェースの利用、サーバへのアクセス、耐タンパ領域へのアクセス、外部メモリへのアクセスのいずれか一以上の動作を行なう。「ローカルインターフェース」とは、端末のもつ外部インターフェースであり、例えば、ＩｒＤＡ（赤外線通信のためのインターフェース）、Ｂｌｕｅｔｏｏｔｈ、その他の無線通信、及び有線通信のためのインターフェースなどが挙げることができる。

【００１９】なお、上記においては、端末と認証モジュールとが容易に分離可能であると書いたが、認証モジュールが端末の回路に対して圧着がされたり半田付けなどがされたりすることにより端末の内部に備えられ容易に分離できないようになっていてもよい。

【００２０】また、上記において、「端末」と記したが、本発明は、携帯可能な機器に限られることなく、端末を使用する代わりにパーソナルコンピュータやワークステーションなどを用いて実施することが可能である。

【００２１】また、本発明は、複数の機器が直列に接続された状態で、一方の端の機器から他方の端の機器が格納するアプリケーションを認証するための処理に応用することも可能である。

【００２２】（実施の形態１）図１は、本発明の実施の形態１に関するアプリケーション認証システムの機能ブロック図である。本実施の形態におけるアプリケーション認証システムは、端末１００と認証モジュール１０１から構成される。

【００２３】端末１００は、アプリケーションをダウンロードするダウンロード部１０２を有する。「アプリケーションをダウンロードする」とは、ダウンロード部１０２の外部からアプリケーションの実行のためのデータを読み込むことである。ここに「アプリケーションの実行のためのデータ」とは、アプリケーションが端末１００により直接実行可能なバイナリデータであれば、そのバイナリデータであり、アプリケーションが端末１００によって解釈実行される言語で記述されたものであれば、その記述である。ダウンロード部は、アプリケーションを実行のためのデータを読み込み、そのデータを保持すること行なう。

【００２４】認証モジュール１０１は、ＴＲＭ部１０３を有している。ＴＲＭ部１０３は、アプリケーションの認証の処理のための情報を耐タンパ領域に保持する。なお、「ＴＲＭ」は、「Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ　Ｍｏｄｕｌｅ」の略である。「アプリケーション」とは、端末１００のダウンロード部１０２にダウンロードされたアプリケーションであり、「アプリケーションの認証」とは、アプリケーションが、信頼のおける者によって発行されたかどうか、不正な動作をしないことの保証を受けているものであるかどうか、あるいは、信頼のおける者から発行されてから後の改ざん、又は、不正な動作をしないことが保証されてから後の改ざんがされていないかどうか、などアプリケーションが不正な動作をしないものであることを確認することである。「アプリケーションの認証の処理」とは、このような確認するための処理である。

【００２５】この認証の処理の方法としては、通常、ＳＨＡ－１（Ｓｅｃｕｒｅ　ＨａｓｈＳｔａｎｄａｒｄ－１）やＭＤ５（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　５）などの、ハッシュ関数（「ハッシュ関数」のかわりに「要約関数」と呼ばれる場合もある）を用いて、アプリケーションの実行のためのデータを入力データとして処理して得られる結果データを求め、それを暗号化したもの（いわゆる「署名」）が用いられる。ここに「ハッシュ関数」とは、入力データを処理して得られる結果データが一致するような二つの異なる入力データを見つけることが計算量的に困難な結果を返す関数である。従って「アプリケーションの認証の処理のための情報」とは、この署名そのもの、あるいは、署名を復号してハッシュ値を得るのに必要な復号鍵である。「耐タンパ領域」とは、認証モジュールの記憶領域であって、その記憶領域

のデータを不正に読み出すことや、その記憶領域のデータを不正に書き換えることが困難な記憶領域である。そのような記憶領域は、例えば、その記憶領域にアクセスするためには、正しい手順を行なわないとアクセスできないハードウェアを経由しなければならないようにしたり、記憶領域に記憶されているデータが暗号化されているようにしたりして実現される。

【００２６】アプリケーションの認証は、端末１００がダウンロード部１０２にダウンロードされたアプリケーションのハッシュ値を求め、そのハッシュ値とともに署名を認証モジュールに提示し、認証モジュール１０１は、ＴＲＭ部１０３に保持された情報により、そのハッシュ値からその署名を生成することができるかどうか、あるいは、そのハッシュ値が署名を復号して得られるハッシュ値と一致するかどうかを調べる。また、端末１００がダウンロード部にダウンロードされたアプリケーションそのものと署名を認証モジュールに提示し、アプリケーションそのものと署名との関係を調べて認証を行なうようにしてもよい。

【００２７】このような構成のアプリケーション認証システムにより、ダウンロード部１０２にダウンロードされたアプリケーションを、認証モジュール１０１のＴＲＭ部１０３に保持された情報により、認証することができるので、不正なアプリケーションがダウンロードされて端末１００内で実行、または、認証モジュール１０１内に格納されてしまうことを防止することができる。

【００２８】図２は、本実施の形態のアプリケーション認証システムの一例を示す。この例において、アプリケーション２０１が格納された状態で認証モジュール１０１をサービス提供会社２００が配布を行なう。認証モジュール１０１を入手した人が端末１００に認証モジュール１０１を装着すると、認証モジュール１０１から端末１００のダウンロード部１０２にアプリケーション２０１がダウンロードされる（矢印２０３）。ダウンロードされたアプリケーション２０２が、認証モジュール１０１のＴＲＭ部に格納された情報により認証がされると、アプリケーション２０２が端末１００内で動作をして、サービス提供会社２００からサービスの提供を受ける（矢印２０４）。

【００２９】図３は、本実施の形態のアプリケーション認証システムの別の例を示す。この例において、サービス提供会社２００は、端末１００のダウンロード部１０２へアプリケーション３０２をダウンロードする（矢印３０３）。アプリケーション３０２に対して、認証モジュール１０１のＴＲＭ部に保持された情報により、認証が行なわれ、不正なアプリケーションでないことが確認されると、認証モジュール１０１へアプリケーション３０１として格納される（矢印３０４）。その後、アプリケーション３０１は、必要に応じて、端末１００のダウンロード部１０２にダウンロードされて端末１００内で実行される。

【００３０】図２と図３とにおいては、端末１００内で実行されるアプリケーションは認証モジュールからダウンロードされるが、端末が接続したサーバよりダウンロードされ、認証モジュールのＴＲＭ部に保持された情報により、認証が行なわれ、不正なアプリケーションでないことが確認されると、そのアプリケーションが端末内で実行されるようになっている例も挙げることができる。

【００３１】なお、「端末」という語を用いたが、これは、携帯電話に代表される携帯可能な端末などに限定されることを意味しない。例えば、家庭用電化製品であってもよいし、いわゆる、情報家電やネット家電と呼ばれるものであってもよい。そのような製品を例示列挙すれば、エアコンディショナ、加湿器、除湿器、空気清浄機、電子レンジ、オーブン、冷蔵庫、食器洗い機、湯沸し器、アイロン、ズボンプレッサー、電気掃除機、洗濯機、乾燥機、電気毛布、電気敷布、照明機器、テレビ受像機、ラジオ受信機、テープレコーダなどのオーディオ機器、カメラ、ＩＣレコーダ、電話機、ファクシミリ送受信機、コピー機、プリンター、スキャナー、パーソナルコンピュータ、などを挙げることができる。

【００３２】（実施の形態２）図４は、本発明の実施の形態２に関するアプリケーション認証システムの機能ブロック図を示し、アプリケーション認証システムは、端末１００と認証モジュール１０１とからなる。端末１００は、ダウンロード部１０２とＴＲＭアクセスライブラリ部４０１とを有する。認証モジュール１０１は、ＴＲＭ部１０３とＴＲＭアクセスライブラリ部認証部４０２とを有する。

【００３３】ダウンロード部１０２は、アプリケーションをダウンロードする。

【００３４】ＴＲＭアクセスライブラリ部４０１は、認証モジュール１０１に自身が認証されることを条件としてアプリケーションの認証のための処理をする。すなわち、ＴＲＭアクセスライブラリ部４０１は、まず、認証モジュール１０１に自身を認証させ、正しく認証された場合に、アプリケーションの認証のための処理を行なう。

【００３５】ＴＲＭアクセスライブラリ部４０１が認証モジュール１０１に自身を認証させる方法としては、端末１００に固有な情報を認証モジュール１０１に出力し、認証モジュール１０１は、出力された情報が耐タンパ領域に格納された情報と適合するかどうかで認証を行なう方法がある。「端末１００に固有な情報」としては、①端末が携帯電話である場合には、その電話番号が挙げられる。また、端末１００に固有な情報の別のものとしては、②端末１００の種類を特定する識別子や、端末１００に付けられた製造番号などの個々の端末ごとに異なるものが付される識別子であってもよい。また、③

端末１００にインストールされているアプリケーションの組み合わせに関する情報を用いてＴＲＭアクセスライブラリ部４０１を認証する方法がある。「端末１００にインストールされているアプリケーション」とは、端末１００内に備えられたアプリケーションを意味し、端末の外部からダウンロードされたアプリケーションや、端末のＲＯＭに格納されたアプリケーションである。この場合、ＴＲＭアクセスライブラリ部４０１は、認証モジュール１０１に、端末１００内にどのアプリケーションがインストールされているかの情報（例えば、インストールされているアプリケーションの識別子など）を出力し、認証モジュール１０１は、出力された情報が、耐タンパ領域に格納された情報と適合するかどうかで認証を行なう。あるいは、不正な端末の情報が耐タンパ領域に格納されており、不正な端末の情報に適合しないかどうかで認証を行なう。

【００３６】上で挙げた❸として例えば、サービスＡとサービスＢとの両方のサービスの提供を受けるための会員になっている者に、新しいサービスＣの提供がされるとする。この場合、サービスＡの提供を受けるためのアプリケーションＡと、サービスＢの提供を受けるためのアプリケーションＢと、が端末１００にインストールされていることを条件としてＴＲＭアクセスライブラリ部４０１が認証モジュール１０１により認証されることにすれば、端末にインストールしているサービスＡとサービスＢとの会員に対して、サービスＣの提供を受けるためのアプリケーションＣを提供することが可能となる。

【００３７】また、ＴＲＭアクセスライブラリ部４０１を識別するための情報を用いてＴＲＭアクセスライブラリ部４０１を認証する方法もある。「ＴＲＭアクセスライブラリ部４０１を識別するための情報」とは、例えば、ＴＲＭアクセスライブラリ部４０１を構成するソフトウェアを識別するための情報であり、そのソフトウェアの名前やバージョン番号やシリアル番号などである。ＴＲＭアクセスライブラリ部４０１は、ＴＲＭアクセスライブラリ部４０１を識別するための情報を認証モジュールに出力し、認証モジュール１０１は、出力された情報が、耐タンパ領域に格納された情報と適合するかどうかで認証を行なう。

【００３８】「アプリケーションの認証のための処理」とは、ダウンロード部１０２にダウンロードされたアプリケーションの認証のための処理である。ＴＲＭアクセスライブラリ部４０１がアプリケーションの認証に関する処理の一部を行なってもよい。また、ＴＲＭアクセスライブラリ部４０１は認証モジュールによって認証されているので、アプリケーションの認証に関する処理の全てを行なってもよい。

【００３９】また、ＴＲＭアクセスライブラリ部４０１の行なう処理は、アプリケーションの認証のための処理に限定される必要はない。例えば、図３６に示すように、更に、ＴＲＭアクセスライブラリ部４０１は、その内部にアプリケーションマネージャとデバイスドライバとを備え、それらの処理を行なうようになっていてもよい。

【００４０】「アプリケーションマネージャ」とは、ダウンロード部１０２にダウンロードされたアプリケーションの起動、終了、サスペンドなど、アプリケーションの動作の制御を行なう機能を提供する。なお、アプリケーションマネージャの別の名称としては、例えば、「アプリケーション制御プログラム」を挙げることができる。

【００４１】「デバイスドライバ」とは、認証モジュールとの入出力を管理するプログラムである。例えば、認証モジュールごとに異なる入出力のための操作の仕様を吸収し、同一のインターフェースの操作によってアプリケーションが入出力を行なえるようにするためのプログラムである。なお、デバイスドライバの別の名称としては、「認証モジュールアクセスプログラム」を挙げることができる。

【００４２】ＴＲＭ部１０３は、ＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持する。「ＴＲＭアクセスライブラリ部認証情報」とは、ＴＲＭアクセスライブラリ部４０１を認証するための情報である。既に説明したように、この情報は、携帯電話番号などの端末１００に固有の情報である場合や、端末１００にインストールされているアプリケーションの組み合わせに関する情報である場合や、ＴＲＭアクセスライブラリ部４０１を識別するための情報である場合などがある。ＴＲＭアクセスライブラリ部認証情報は耐タンパ領域に保持されるため、携帯電話番号、端末１００にインストールされているアプリケーションを識別するための情報、ＴＲＭアクセスライブラリ部４０１を識別するための情報が暗号化されて保持されている場合もある。

【００４３】ＴＲＭアクセスライブラリ部認証部４０２は、ＴＲＭアクセスライブラリ部認証情報に基づいて端末のＴＲＭアクセスライブラリ部４０１を認証する。すなわち、ＴＲＭアクセスライブラリ部４０１から認証モジュールに出力される認証のための情報と、ＴＲＭ部１０３に保持されるＴＲＭアクセスライブラリ部認証情報と、により、ＴＲＭアクセスライブラリ部４０１を認証することを行なう。

【００４４】図５は、アプリケーションを本実施の形態のアプリケーション認証システムにおいて、アプリケーションの認証の方法を説明するための図である。図４と図５とに示されたアプリケーション認証システムの違いは、図５の端末１００のダウンロード部１０２が、改ざんのないことを認証するために用いる情報である署名が付加されたアプリケーションをダウンロードする点と、端末１００が署名認証情報出力部５０１をさらに有する点と、認証モジュール１０１が署名認証情報入力部５０

２と、署名認証部５０３とをさらに有する点である。

【００４５】「改ざんのないことを認証するために用いる情報である署名」とは、アプリケーションが改ざんされていないことを確認するための情報である。図６は、アプリケーションと署名の関係とを示す。アプリケーション本体６０１をデータとみなしてそれに対して、ＳＨＡ－１やＭＤ５などのハッシュ関数を適用して得られる値を暗号化したものが署名６０２である。署名６０２を用いてアプリケーション本体が改ざんされていないことを確認するには、まず、署名を復号してハッシュ値を得る。次に、アプリケーション本体に対してハッシュ関数を適用し、得られる値が、署名を復号して得られるハッシュ値と同じであるかどうかを確認する。あるいは、アプリケーション本体にハッシュ関数を適用してハッシュ値を得て、それに対して暗号化を行い、得られたものが署名と同じであるかどうかを確認する。前者の方法は、例えば、署名が公開鍵暗号化方式を用いる場合に普通に利用される方法であり、署名は、ハッシュ値を署名を行なう者の秘密鍵によって暗号化され、アプリケーション本体が改ざんされていないことを確認する時に、署名を行なった者の秘密鍵に対応する公開鍵によって復号される。後者の方法は、例えば、アプリケーション本体が改ざんされていないことを確認する者が署名を行なった者の秘密鍵を知っている場合や、共通鍵暗号化方式が用いられる場合に使用される。

【００４６】本実施の形態において、ＴＲＭアクセスライブラリ部４０１は、自身を認証モジュールに認証させた後で、ダウンロード部１０２にダウンロードされたアプリケーションの認証のための処理の一部である処理、すなわち、ダウンロード部１０２にダウンロードされたアプリケーションから署名認証用ダイジェストを生成することを行なう。「署名認証用ダイジェスト」とは、上に挙げたＳＨＡ－１やＭＤ５などのハッシュ関数によるハッシュ値である。

【００４７】署名認証情報出力部５０１は、ＴＲＭアクセスライブラリ部４０１で生成された署名認証用ダイジェスト５０４と署名５０５とを含む署名認証情報５０６を認証モジュールに出力する。ここに「署名５０５」とは、ダウンロード部１０２にダウンロードされたアプリケーションに付加された署名である。

【００４８】署名認証情報入力部５０２は、署名認証情報出力部５０１から出力された署名認証情報５０６を入力する。

【００４９】署名認証部５０３は、署名認証情報入力部５０２から入力される署名認証用ダイジェストと署名とに基づいて署名の検証を行なう。検証の方法としては、例えば、署名が公開鍵暗号化方式の秘密鍵で暗号化されている場合には、その秘密鍵に対応する公開鍵で復号し、その復号の結果と署名認証用ダイジェストとを比較して等しいかどうかで認証を行なう。あるいは、耐タンパ領域に共通鍵を保持しておき、その共通鍵で署名を復号して署名認証用ダイジェストと比較する方法、あるいは、その秘密鍵を耐タンパ領域に保持して、その秘密鍵で署名認証用ダイジェストを暗号化して署名と比較する方法がある。

【００５０】図７は、端末１００の動作を説明するフローチャートである。このフローチャートの処理を行なう前提として、ＴＲＭアクセスライブラリ部４０１は、認証モジュールにより認証されているとする。ステップＳ７０１において、ダウンロード部１０２にアプリケーションをダウンロードする。ステップＳ７０２において、ダウンロードしたアプリケーションより署名認証用ダイジェストを、ＴＲＭアクセスライブラリ部４０１で生成する。ステップＳ７０３において、ステップＳ７０２で求められた署名認証用ダイジェストとダウンロードされたアプリケーションに付加された署名とを含む署名認証情報５０６を、署名認証情報出力部５０１より認証モジュール１０１に出力する。

【００５１】図８は、認証モジュール１０１の署名認証情報入力部５０２と署名認証部５０３との動作を説明するフローチャートである。このフローチャートの処理を行なう前提として、ＴＲＭアクセスライブラリ部４０１は、認証モジュールにより認証されているとする。このために、例えば、ＴＲＭアクセスライブラリ部認証部４０２は認証の結果を認証モジュール１０１内に設定しておくものとし、図８のフローチャートの処理を行なうときには、その設定された認証の結果を参照して、ＴＲＭアクセスライブラリ部４０１が認証されている場合に限り、図８のフローチャートの処理を行なうようにする方法がある。ステップＳ８０１において、署名認証情報５０６を、署名認証情報入力部５０２により入力する。ステップＳ８０２において、署名認証用ダイジェスト５０４と署名５０５とに基づいて署名の検証を行なう。署名の検証の方法については、上で説明した通りである。

【００５２】本実施の形態においては、ＴＲＭアクセスライブラリ部４０１は、認証モジュール１０１によって認証がされたことを条件にして、ダウンロード部１０２にダウンロードされたアプリケーションの署名認証用ダイジェストを生成し、生成された署名用認証用ダイジェストが認証モジュール１０１に入力されるので、署名認証用ダイジェストは信頼のおけるものであり、ダウンロード部１０２にダウンロードされたアプリケーションの認証を認証モジュール１０１が行なうことができる。

【００５３】（実施の形態３）図９は、本発明の実施の形態３にかかわる認証モジュール１０１の機能ブロック図を示す。本実施の形態は、実施の形態２における署名認証情報による認証方法をより具体的にしたものであり、実施の形態２の認証モジュール１０１が、署名由来ダイジェスト生成情報取得部９０１と、署名由来ダイジェスト生成部９０２と、をさらに有している。

【００５４】署名由来ダイジェスト生成情報取得部９０１は、署名認証情報入力部５０２から入力される署名を利用して署名由来ダイジェストを生成するための署名由来ダイジェスト生成情報を取得する。署名が、アプリケーション本体のハッシュ値を暗号化したものであれば、「署名由来ダイジェスト生成情報」は、暗号化したものを復号する復号鍵である。暗号化として公開鍵暗号化方式が使用されている場合には、アプリケーション本体のハッシュ値を暗号化するために用いられた秘密鍵に対応する公開鍵が署名由来ダイジェスト生成情報となる。この公開鍵は、認証モジュールに保持されていてもよい。また、端末１００などを経由して適当なサーバより取得するようになっていてもよい。

【００５５】署名由来ダイジェスト生成部９０２は、署名認証情報入力部から入力された署名９０３と、署名由来ダイジェスト生成情報取得部に保持された署名由来ダイジェスト生成情報と、を利用して署名由来ダイジェスト９０５を生成する。すなわち、署名由来ダイジェスト生成情報が公開鍵であれば、署名９０３をその公開鍵で復号してアプリケーション本体のハッシュ値である署名由来ダイジェスト９０５を生成する。

【００５６】署名認証部５０３は、署名由来ダイジェスト生成部９０２で生成された署名由来ダイジェスト９０５と、署名認証情報入力部５０２から入力された署名認証用ダイジェスト９０４と、に基づいて認証を行なう。すなわち、署名由来ダイジェスト９０５と署名認証用ダイジェスト９０４とを比較し、同じものであれば、ダウンロード部１０２にダウンロードされたアプリケーションを認証し、異なるものであれば、認証しない。

【００５７】図１０は、本実施の形態における署名認証情報入力部５０２と、署名由来ダイジェスト生成情報取得部９０１と、署名由来ダイジェスト生成部９０２と、署名認証部５０３との動作を説明するフローチャートである。このフローチャートの処理を行なう前提として、ＴＲＭアクセスライブラリ部４０１は、認証モジュール１０１により認証されているとする。このためには例えば、ＴＲＭアクセスライブラリ部認証部４０２は認証の結果を認証モジュール１０１内に設定しておくものとし、図１０のフローチャートの処理を行なうときには、その設定された認証の結果を参照して、ＴＲＭアクセスライブラリ部４０１が認証されている場合に限り、図１０のフローチャートの処理を行なうようにする方法がある。ステップＳ１００１において、署名認証情報５０６を、署名認証情報入力部５０２により入力し、署名９０３と署名認証用ダイジェスト９０４を得る。ステップＳ１００２において、署名由来ダイジェスト生成情報を、署名由来ダイジェスト生成情報取得部９０１により取得する。ステップＳ１００３において、署名９０３と署名由来ダイジェスト生成情報から、署名由来ダイジェスト生成部９０２において、署名由来ダイジェスト９０５を生成する。ステップＳ１００４において、署名由来ダイジェスト９０５と署名認証用ダイジェスト９０４に基づいて、署名認証部５０３において認証を行なう。

【００５８】（実施の形態４）図１１は、本発明の実施の形態４に関するアプリケーション認証システムの機能ブロック図を示す。本実施の形態においては、実施の形態２または実施の形態３におけるアプリケーション認証システムの端末がさらに認証モジュール認証部１１０１を有している。

【００５９】認証モジュール認証部１１０１は、認証モジュール１０１を認証する。この認証の方法としては、図１２に示したフローチャートに示した方法がある。この方法を用いるにあたっては、認証モジュールに対して公開鍵暗号化方式の秘密鍵とそれに対応する公開鍵が生成され、認証モジュールは、その秘密鍵を格納していることを前提とする。ステップＳ１２０１において、認証モジュール認証部１１０１は、乱数を発生させる。ステップＳ１２０２において、認証モジュール１０１の持つ公開鍵によりステップＳ１２０１で発生させた乱数を暗号化する。ステップＳ１２０３において、認証モジュール１０１に、ステップＳ１２０２で暗号化した乱数を入力し、復号するように要求する。ステップＳ１２０４において、認証モジュール１０１からの復号の結果を受け取り、ステップＳ１２０５において、ステップＳ１２０１で発生させた乱数とステップＳ１２０４で受け取った復号の結果が等しいか判断する。別の方法としては、認証モジュール認証部１１０１は、発生させた乱数を認証モジュール１０１に入力し、その乱数を認証モジュール１０１の秘密鍵で暗号化するように要求する方法がある。認証モジュール認証部１１０１は、その暗号化の結果を得て、認証モジュール１０１の公開鍵で復号し、認証モジュール１０１に入力した乱数と等しいかどうかを判断する。

【００６０】このように、端末１００が認証モジュール１０１を認証するための認証モジュール認証部１１０１を有することにより、端末１００が認証モジュール１０１を認証することができ、端末１００内で動作するアプリケーションが機密性の高い情報（プライバシー情報、Ｅ－コマース（ＥＣ）のログ、銀行取引における口座残高など）を認証モジュール１０１に書き込む際に、認証モジュール１０１が正当なものであるかどうかを確認することができる。

【００６１】（実施の形態５）図１３は、本発明の実施の形態５に関するアプリケーション認証システムの機能ブロック図を示す。本実施の形態は、実施の形態４におけるアプリケーション認証システムのＴＲＭアクセスライブラリ部４０１が、アプリケーション利用リソース情報保持手段１３０１をさらに有している形態である。

【００６２】アプリケーション利用リソース情報保持手段１３０１は、アプリケーション利用リソース情報を保

持する。「アプリケーション利用リソース情報」とは、認証されたアプリケーションに対して利用を認めるリソースに関する情報である。「認証されたアプリケーション」とは、ダウンロード部１０２にダウンロードされたアプリケーションであって、ＴＲＭアクセスライブラリ部４０１による認証のための処理が行なわれ、正しく認証されたアプリケーションである。「リソース」とは、アプリケーションが利用するアプリケーションの外部の資源である。リソースには、端末１００およびそれに装着された認証モジュール１０１の資源であるローカルリソースと、それ以外のリソース、例えば、端末１００の通信先であるサーバの資源であるリソースがある。ローカルリソースには、メモリの使用、ファイルの使用、ＩｒＤＡの使用、Ｂｌｕｅｔｏｏｔｈの使用，通信の使用、ＴＲＭの使用、アプリケーションの使用、非接触／接触ＩＣカードＩ／Ｆの使用などの種類がある。また、ローカルリソースのうち、メモリの使用などの場合には、使用できるメモリの量やメモリの番地などの範囲に関するものもある。また、使用できる時間という範囲も挙げることができる。

【００６３】図１４は、アプリケーション利用リソース情報を例示している。図１４において、アプリケーション利用リソース情報１４００は、メモリの使用１４０１、ファイルの使用１４０２、ＩｒＤＡの使用１４０３、Ｂｌｕｅｔｏｏｔｈの使用１４０４、通信の使用１４０５、ＴＲＭの使用１４０６、アプリケーションの使用１４０７、非接触／接触ＩＣカードＩ／Ｆの使用１４０８、動作１４０９、使用日時１４１０などの項目から成っている。

【００６４】メモリの使用１４０１の項目としては、例えば、メモリとして使用可能な量、使用可能な範囲のアドレス、書き込みができる回数、読み出しができる回数、メモリが使用可能な日時、使用不可能な日時などを挙げることができる。フラッシュメモリにとっては、書き込みは負担のかかる操作であるので、メモリの書き込みの回数を制限することには特に意味がある。

【００６５】ファイルの使用１４０２の項目としては、端末１００の持つファイルや認証モジュール１０１などの端末１００に接続された外部のメモリの持つファイルに対するアクセスの制限を記述するものが挙げられ、例えば、アクセス可能なディレクトリ名、アクセス可能なファイル名、アクセス可能なファイルの種類（例えば、ファイルの拡張子によって指定される）、使用可能な日時、使用不可能な日時などがある。

【００６６】ＩｒＤＡの使用１４０３は、端末１００の持つ赤外線通信の機能の使用を認めるかどうかを表す項目であり、その機能が使用可能／不可能な時刻、使用可能なトータル時間、使用回数などを挙げることができる。

【００６７】Ｂｌｕｅｔｏｏｔｈの使用１４０４は、端末１００の持つＢｌｕｅｔｏｏｔｈによる通信の機能の使用を認めるかどうかを表す項目であり、その機能が使用可能な時刻、使用可能なトータル時間、使用回数のほかに、使用可能な電波の強度、ローミング回数、使用可能／不可能な日時、などを挙げることができる。使用可能な電波の強度を指定することにより、通信可能な距離を指定することができる。

【００６８】通信の使用１４０５は、サーバなどとの通信の機能の使用を認めるかどうかを表す項目であり、その機能が使用可能／不可能な時刻、使用可能なトータル時間、使用回数、使用可能な電波の強度、ローミング回数のほかに、アクセス可能なサーバなどを挙げることができる。アクセス可能なサーバは、ＩＰアドレスによるアドレスの指定、ドメイン名による指定、あるいは、メールサーバやＦＴＰサーバなどのサーバの機能あるいはサーバとの通信のプロトコルによる指定により、アプリケーションがサーバなどを利用できるかどうかが指定される。

【００６９】ＴＲＭの使用１４０６は、認証モジュール１０１などの耐タンパ領域へのアクセスを認めるかどうかを表す項目であり、その耐タンパ領域へのアクセスができる日時、アクセスができない日時、アクセス回数や、耐タンパ領域を持つＩＣカード内で動作するカードアプリケーションであって、アクセス可能なカードアプリケーション、利用可能なＩＣカードコマンドの種類などが挙げられる。

【００７０】アプリケーションの使用１４０７は、アプリケーションが連携可能な他のアプリケーションを指定する項目である。例えば、アドレス帳やメール、スケジューラ、ゲームなどである。また、他のアプリケーションと連携することが可能な日時も含まれていてもよい。端末１００が携帯電話である場合には、電話通信時にアプリケーションが通話と並行して動作することを認めるかどうか、通話の開始時に停止あるいは終了しなければいけないかどうかを指定するようにしてもよい。

【００７１】接触／非接触ＩＣカードＩ／Ｆの使用１４０８は、端末１００と交信が可能な接触／非接触ＩＣカードやＩＣカードリーダライタと交信するためのインターフェースの使用を認めるかどうかの項目である。そのインターフェースが使用可能な時刻、使用可能なトータルの時間、使用可能／不可能な回数、使用可能Ｉ／Ｆ（Ｔｙｐｅ　Ａ、Ｔｙｐｅ　Ｂ、Ｔｙｐｅ　Ｃなど）、利用可能なＩＣカードコマンドの種類などが挙げられる。

【００７２】使用日時１４１０は、アプリケーションが動作可能な日時を指定する。あるいは、アプリケーションの動作を停止すべき日時を指定する。

【００７３】ダウンロード部１０２にダウンロードされたアプリケーションが、リソースを使用する際には、ＴＲＭアクセスライブラリ部４０１に対してリソースに使

用の要求を出し、ＴＲＭアクセスライブラリ部４０１は、アプリケーション利用リソース情報保持手段１３０１に保持されているアプリケーション利用リソース情報を参照し、要求されたリソースが使用可能かどうかを判断し、もし、使用可能であれば、その要求されたリソースをアプリケーションに使用させる。

【００７４】アプリケーション利用リソース情報は、ダウンロード部１０２にダウンロードされるアプリケーションとともにダウンロードされて、アプリケーション利用リソース情報保持手段１３０１に保持されるようになっていてもよい。図１５は、アプリケーションとともにアプリケーション利用リソース情報がダウンロードされるデータを模式的に表現した図である。まず、アプリケーション本体であるアプリケーションデータ１５０１があり、アプリケーションデータ１５０１を認証するための署名であるアプリケーションデータ署名データ１５０２が続き、その後ろに、アプリケーション利用リソース情報１５０３があり、アプリケーション利用リソース情報を認証するためのアプリケーション利用リソース情報署名データ１５０４がある。アプリケーション利用リソース情報１５０３には、符号１５０５が付された部分のように、「ＩｒＤＡ　１」により、ＩｒＤＡが使用可能であり、「Ｂｌｕｅｔｏｏｔｈ　０」により、Ｂｌｕｅｔｏｏｔｈは使用不可、であることなどが表現される。

【００７５】また、アプリケーション利用リソース情報は、認証モジュール１０１に格納され、必要に応じて読み出され、アプリケーション利用リソース情報保持手段１３０１により保持されるようになっていてもよい。

【００７６】このように、アプリケーション利用リソース情報保持手段１３０１をＴＲＭアクセスライブラリ部４０１が有する構成により、ダウンロードされたアプリケーションが使用可能な資源を制限することが可能となる。これにより、アプリケーション利用リソース情報をアプリケーションの製作者やサービス提供者などに対して発行して対価を得るというビジネスを行なうことができる。このローカルリソースの許可の制御には、アプリケーション利用リソース情報を用いることができ、特定のアプリケーションに対してローカルリソースの利用を細かく許可／不許可にすることができる。ローカルリソースの許可を行なう場合には、アプリケーション利用リソース情報の発行者に使用料を支払うようにすれば、アプリケーション利用リソース情報の発行による商取引が可能となる。また、端末１００の利用者は、対価を支払うことにより、端末１００にダウンロードされたアプリケーションのリソースの使用に対する制限がより少ないアプリケーション利用リソース情報を入手することが可能となり、端末１００の利用者を相手とする商取引も実現できる。

【００７７】なお、実施の形態２ないし実施の形態５において、ダウンロード部１０２が使用許諾書をダウンロードしてもよい。「使用許諾書」とは、ダウンロードアプリケーションの署名付きのアプリケーション利用リソース情報である。「ダウンロードアプリケーション」とは、ダウンロード部１０２にダウンロードされたアプリケーションである。「署名付きのアプリケーション利用リソース情報」とは、アプリケーション利用リソース情報にそのアプリケーション利用リソース情報の署名を付したものである。アプリケーション利用リソース情報は、ダウンロードされたアプリケーションが端末１００や認証モジュール１０１のリソースを使用するための許可証であるので、アプリケーション利用リソース情報の真正性を保証することは重要であり、そのために署名をアプリケーション利用リソース情報に付けるようにする。

【００７８】なお、ダウンロードされたアプリケーションの署名の検証と、アプリケーション利用リソース情報の署名の検証とは、同時に行なわれても、異なる時に行なわれてもよい。例えば、最初にアプリケーションの署名の検証が行なわれ、アプリケーションが動作し、リソースにアクセスをしたときに、アプリケーション利用リソース情報の署名の検証が行われ、真正なものであることを確認してリソースのアクセスが許されるかどうかを判断するようにしてもよい。また、ダウンロードされたアプリケーションの署名とアプリケーション利用リソース情報の署名の作成者は、同じであっても異なっていてもよい。署名の作成者が異なることがあり得る理由は、アプリケーションの作成者とアプリケーション利用リソース情報の発行者とは異なり、前者が後者に対してリソースの利用の許可を申請して、後者よりアプリケーション利用リソース情報の発行を受けることがあるからである。なお、リソースの利用の許可の申請の際に、対価の収受が行なわれてもよい。

【００７９】また、使用許諾書のアプリケーション利用リソース情報に、アプリケーションが、リソースをアクセスすることができる時間的限度を示す期限日情報が含まれている場合には、その期限日情報に基づいて認められる時間的情報がすでに期限切れである場合には、ダウンロード部１０２は、使用許諾書をダウンロードし、使用許諾書を更新するようにしてもよい。

【００８０】また、ダウンロードされたアプリケーションの実行時、又は／及び、アプリケーションの認証時に使用許諾書をダウンロードするようにしてもよい。使用許諾書のダウンロードは、端末１００が通信できるサーバより行なってもよい。また、認証モジュール１０１より行なってもよい。

【００８１】また、ダウンロード部１０２は、サーバよりダウンロードした使用許諾書を保持し続けることも考えられるが、この場合、使用許諾書がサーバ内において更新されている場合があり、ダウンロード部１０２で保持されている使用許諾書が失効している可能性がある。

そこで、ダウンロード部１０２は、ダウンロードされたアプリケーションの実行時、又は／及び、アプリケーションの認証時に、ダウンロードされた使用許諾書の有効性をサーバに問い合わせるようにしてもよい。

【００８２】また、ダウンロード部１０２は、ダウンロード部１０２あるいは端末１００の他の部が、使用許諾書の内容をサーバに対してオンラインにて問い合わせて、アプリケーションのリソースの利用が許可されているかどうかを問い合わせるようになっていてもよい。

【００８３】（実施の形態６）図１６は、本発明の実施の形態６に関するアプリケーション認証システムの機能ブロック図を示す。本実施の形態は、実施の形態４または実施の形態５のアプリケーション認証システムの端末１００のＴＲＭアクセスライブラリ部４０１がアプリケーション利用リソース情報出力手段１６０１を有する。

【００８４】アプリケーション利用リソース情報出力手段１６０１は、認証モジュール認証部１１０１による認証がされた認証モジュールに対してアプリケーション利用リソース情報を出力する。

【００８５】本実施の形態において、認証モジュール１０１のＴＲＭ部１０３は、アプリケーション利用リソース情報出力手段１６０１から出力されたアプリケーション利用リソース情報を耐タンパ領域に書き換え可能に保持することを行なう。

【００８６】このように耐タンパ領域に保持されたアプリケーション利用リソース情報は、必要に応じて端末１００に読み込まれ、ダウンロード部１０２にダウンロードされたアプリケーションが資源を使用しようとする際に、その資源が使用できるかどうかを判断するために参照される。

【００８７】このように、端末１００のＴＲＭアクセスライブラリ部４０１がアプリケーション利用リソース情報出力手段１６０１を有し、アプリケーション利用リソース情報出力手段１６０１により出力されたアプリケーション利用リソース情報をＴＲＭ部１０３が保持することにより、認証モジュール１０１に保持された状態でアプリケーション利用リソース情報が提供された後でも、必要に応じてアプリケーション利用リソース情報を書き換えることができる。例えば、アプリケーション利用リソース情報の有効期限を書き換えることなどが可能となる。また、例えば、サービスの提供者やサービスの利用者が対価を支払うことにより、耐タンパ領域が保持するアプリケーション利用リソース情報を、アプリケーションの使用可能な資源を制限することが少ないものに更新することができる。書き換えは、あらかじめ署名認証情報入力部５０２によって認証されたＴＲＭアクセスライブラリ部４０１により行なわれるので、不正な書き換えを防止することができる。

【００８８】（実施の形態７）図１７は、本発明の実施の形態７に関するアプリケーション認証システムの機能

ブロック図を示す。本実施の形態は、実施の形態５または実施の形態６におけるアプリケーション認証システムの端末１００がアプリケーション利用リソース情報ダウンロード部１７０１を有している。

【００８９】アプリケーション利用リソース情報ダウンロード部１７０１は、署名１７０３が付されたアプリケーション利用リソース情報１７０２をダウンロードする。このダウンロードは、図１５に示すようにダウンロード部１０２にダウンロードされるアプリケーションとともにダウンロードされてもよい。また、ダウンロード部１０２にダウンロードされたアプリケーションとは別にダウンロードされてもよい。例えば、先にアプリケーションをダウンロードしておき、そのアプリケーションが資源にアクセスしようとするときに、アプリケーション利用リソース情報がダウンロードされるようになっていてもよい。

【００９０】本実施の形態において、ＴＲＭアクセスライブラリ部４０１が、アプリケーション利用リソース情報ダウンロード部１７０１にダウンロードされたアプリケーション利用リソース情報１７０２に付された署名１７０３を認証するようにしてもよい。ＴＲＭアクセスライブラリ部４０１は、認証モジュール１０１によって認証されるので、正しく認証されたＴＲＭアクセスライブラリ部４０１により、アプリケーション利用リソース情報１７０２の署名１７０３を認証した結果は認証モジュール１０１にとって信頼できるものになっている。したがって、このように認証されたアプリケーション利用リソース情報１７０２に従って、ダウンロードされたアプリケーションが認証モジュール１０１へアクセスを許しても不正な操作は発生しないことが保証される。

【００９１】（実施の形態８）図１８は、本発明の実施の形態８に関するアプリケーション認証システムの機能ブロック図を示す。本実施の形態は、実施の形態５または実施の形態６におけるアプリケーション認証システムの端末１００がアプリケーション利用リソース情報ダウンロード部１７０１と、アプリケーション利用リソース情報署名認証情報出力部１８０１を有し、認証モジュール１０１がアプリケーション利用リソース情報署名認証情報入力部１８０２と、アプリケーション利用リソース情報署名認証部１８０３とを有している。本実施の形態は、実施の形態７において、ＴＲＭアクセスライブラリ部４０１がアプリケーション利用リソース情報１７０２に付された署名１７０３を認証するかわりに、認証モジュールによって署名１７０３を認証する形態である。

【００９２】アプリケーション利用リソース情報ダウンロード部１７０１は、署名１７０３が付されたアプリケーション利用リソース情報１７０２をダウンロードする。

【００９３】本実施の形態において、ＴＲＭアクセスライブラリ部４０１は、アプリケーション利用リソース情

報ダウンロード部１７０１にダウンロードされたアプリケーション利用リソース情報１７０２から署名認証用ダイジェストを生成し、アプリケーション利用リソース情報署名認証情報出力部１８０１は、生成された署名認証用ダイジェストと、署名１７０３とを含む署名認証情報１８０６を認証モジュールに出力する。

【００９４】アプリケーション利用リソース情報署名認証情報入力部１８０２は、アプリケーション利用リソース情報署名認証情報出力部１８０１から出力された署名認証情報１８０６を入力する。署名認証情報１８０６は、ＴＲＭアクセスライブラリ部４０１で生成された署名認証用ダイジェスト１８０４と、アプリケーション利用リソース情報１７０２に付された署名１７０３である署名１８０５と、を含む。

【００９５】アプリケーション利用リソース情報署名認証部１８０３は、アプリケーション利用リソース情報署名認証情報入力部１８０２から入力される署名認証用ダイジェスト１８０４と署名１８０５とに基づいて署名の検証を行なう。

【００９６】図１９は、本実施の形態における端末１００の動作を説明するフローチャートである。ステップＳ１９０１において、アプリケーション利用リソース情報１７０２より、ＴＲＭアクセスライブラリ部４０１にて、署名認証用ダイジェスト１８０４を生成する。ステップＳ１９０２において、署名認証用ダイジェスト１８０４と署名１８０５とを含む署名認証情報１８０６を、アプリケーション利用リソース情報署名認証情報出力部１８０１により、認証モジュール１０１に出力する。ステップＳ１９０３において、認証モジュール１０１より認証結果を受け取ることを行なう。

【００９７】図２０は、本実施の形態における認証モジュール１０１の動作を説明するフローチャートである。ステップＳ２００１において、署名認証情報１８０６を、アプリケーション利用リソース情報署名認証情報入力部１８０２により入力する。ステップＳ２００２において、署名認証用ダイジェスト１８０４と署名１８０５とに基づいて署名１８０５の署名の検証を、アプリケーション利用リソース情報署名認証部１８０３において行なう。ステップＳ２００３において、検証の結果を端末１００へ返す。

【００９８】このような実施の形態において、認証モジュール１０１によって認証されたＴＲＭアクセスライブラリ部４０１により生成された署名用認証用ダイジェストに基づいてアプリケーション利用リソース情報１７０２の署名が認証されるので、その認証の結果は信頼できるものになる。また、アプリケーション利用リソース情報署名認証部１８０３での認証を、暗号化に基づかずに、認証モジュール１０１のＴＲＭ部に格納された署名に適合するかどうかで認証することも可能になるので、認証を簡単な手間で行なうことができる。

【００９９】（実施の形態９）本発明の実施の形態９は、認証モジュール内で動作する認証モジュール内アプリケーションが、ＴＲＭアクセスライブラリ部が認証モジュールによって認証されていることを条件に、端末内で動作するアプリケーションからのアクセスを受け入れることを特徴とする。

【０１００】図２１は、本実施の形態に関するアプリケーション認証システムの機能ブロック図を示す。本実施の形態は、実施の形態２ないし実施の形態３におけるアプリケーション認証システムの端末１００が端末アプリケーション保持部２１０１を有し、認証モジュール１０１は、認証モジュール内アプリケーション保持部２１０３を備えるＴＲＭ部１０３を有する。

【０１０１】端末アプリケーション保持部２１０１は、認証モジュール１０１のＴＲＭ部にアクセスをする端末アプリケーション２１０２を保持する。「端末アプリケーション２１０２」とは、端末１００の内部で実行されるアプリケーションである。そのアプリケーションは、ダウンロード部１０２によってダウンロードされたアプリケーションであってもよく、また、端末のＲＯＭに保持されているアプリケーションであってもよい。「保持する」とは、端末アプリケーション２１０２を実行可能にすることである。したがって、端末アプリケーション保持部２１０１は、端末アプリケーション２１０２を実行させるために、端末アプリケーション２１０２の全部または一部をロードする端末１００の書き換え可能なメモリ領域により実現される。

【０１０２】認証モジュール内アプリケーション保持部２１０３は、認証モジュール内アプリケーション２１０４を保持する。「認証モジュール内アプリケーション２１０４」とは、認証モジュール１０１内で動作するアプリケーションである。認証モジュール１０１がＩＣカードであれば、認証モジュール内アプリケーション２１０４はカードアプリケーションとなる。「保持する」とは、認証モジュール内アプリケーション２１０４を実行可能にすることである。したがって、認証モジュール内アプリケーション保持部２１０３は、認証モジュール内アプリケーション２１０４を実行させるために、認証モジュール内アプリケーション２１０４の全部または一部をロードする認証モジュールの書き換え可能なメモリ領域により実現される。

【０１０３】本実施の形態において、認証モジュール内アプリケーション２１０４は、ＴＲＭアクセスライブラリ部認証部４０２によるＴＲＭアクセスライブラリ部４０１の認証を条件として端末アプリケーション２１０２からのアクセスを受け入れて動作する。このために、認証モジュール内にＴＲＭアクセスライブラリ部４０１が認証されたかどうかを示す値を格納しておき、図２２に示すように、ステップＳ２２０１において、その値自身あるいは、そのような値が存在するかどうかを調べてＴ

ＲＭアクセスライブラリ部４０１の認証が成功したかどうかを判定する。もし、認証が成功していれば、ステップＳ２２０２に移行し、端末アプリケーション２１０２からのアクセスを受け入れる。ステップＳ２２０１の判定は、認証モジュール内アプリケーション２１０４で行なう場合と、認証モジュール内アプリケーション２１０４以外において行なう場合がある。認証モジュール内アプリケーション２１０４で行なう場合は、認証モジュール内アプリケーション２１０４が起動してから、端末アプリケーション２１０２がアクセスするまでの間に、ＴＲＭアクセスライブラリ部４０１が認証されたかどうかを示す値を見て、判断することになる。認証モジュール内アプリケーション２１０４以外においてステップＳ２２０１の判定を行なう場合は、認証モジュール内アプリケーション２１０４が起動される際に、ＴＲＭアクセスライブラリ部４０１が認証されたかどうかを示す値が確認される。

【０１０４】認証モジュール１０１がＩＣカードである場合には、認証モジュール内アプリケーション２１０４を起動するのは、カードマネージャであるので、カードマネージャが認証モジュール内アプリケーション２１０４を起動するかどうかを、ＴＲＭアクセスライブラリ部４０１が認証されたかどうかを示す値を見て判断することになる。また、認証モジュール１０１の端末とのインターフェース部分（図２１において図示せず）が、端末アプリケーション２１０２から認証モジュール内アプリケーション２１０４へのアクセスを許可するかどうかを決める際に、ＴＲＭアクセスライブラリ部４０１が認証されたかどうかを示す値を見て判断するようにしてもよい。

【０１０５】また、認証モジュール内アプリケーション２１０４が、端末アプリケーション２１０２からのアクセスを受け付けるたびに、ＴＲＭアクセスライブラリ部４０１が認証されたかどうかを示す値を見て、そのアクセスを受け入れて動作するかどうかを決定するようにしてもよい。図２３は、このような場合の認証モジュール内アプリケーションの動作を説明するフローチャートである。ステップＳ２３０１において、端末アプリケーション２１０２からのアクセスを、認証モジュール内アプリケーション２１０４で受け付ける。ステップＳ２３０２において、ＴＲＭアクセスライブラリ部４０１が認証されたかどうかを示す値を、認証モジュール内アプリケーション２１０４がチェックして、ＴＲＭアクセスライブラリ部４０１の認証が成功したかどうかを判断し、もし、その認証が成功していれば、ステップＳ２３０３において、端末アプリケーション２１０２からのアクセスを受け入れて動作する。

【０１０６】図２４は、ＴＲＭアクセスライブラリ部４０１が認証されたかどうかを示す値をＴＲＭ部１０３に格納するようにした形態を示す。ＴＲＭ部１０３は、認

証結果識別子生成手段２４０１を有している。認証結果識別子生成手段２４０１は、ＴＲＭアクセスライブラリ部認証部４０２によるＴＲＭアクセスライブラリ部４０１の認証の成功を条件として認証結果識別子２４０２を生成する。認証モジュール内アプリケーション２１０４は、認証結果識別子２４０２の存在を条件として、端末アプリケーション２１０２からのアクセスを受け入れる。

【０１０７】なお、認証結果識別子２４０２は、ＴＲＭアクセスライブラリ部認証部４０２によるＴＲＭアクセスライブラリ部４０１の認証の成功を示すだけではなく、認証の失敗を示す内容を持つものであってもよい。この場合には、認証結果識別子生成手段２４０１は、ＴＲＭアクセスライブラリ部認証部４０２によるＴＲＭアクセスライブラリ部４０１の認証の成功／失敗に応じた内容を持つ認証結果識別子２４０２を生成する。また、認証モジュール内アプリケーション２１０４は、認証結果識別子２４０２の内容を見て、認証が成功したかどうかを判断する。

【０１０８】図２５は、認証モジュール１０１がＩＣカードである場合における、認証結果識別子の実現方法を示す。図２５において、ＴＲＭアクセスライブラリ部４０１を認証するのがカードアプリケーションＡ（２５０１）であり、ＴＲＭアクセスライブラリ部４０１が認証されると、書き換えが可能なメモリ領域、例えば、ＲＡＭ領域２５０３に認証結果識別子を設定する。図２５において、旗の印が認証結果識別子を模式的に表現している。ＲＡＭ領域２５０３は、カードアプリケーションＡ（２５０１）は読み書きすることができるが、ＩＣカード内のアプリケーション間で、それぞれ悪影響を及ぼし合わないよう、各アプリケーションを独立して起動させるためのファイアウォール機能により、別のカードアプリケーションＢ（２５０２）は、ＲＡＭ領域２５０３に直接アクセスすることができない。そこで、カードアプリケーションＡ（２５０１）が相手先を指定してインターフェースを公開できる公開インターフェース（Ｓｈａｒａｂｌｅ　Ｉｎｔｅｒｆａｃｅ）機能を利用して公開インターフェース２５０４を提供し、この公開インターフェース２５０４を通して、端末アプリケーション２４０２からアクセスがされたカードアプリケーション２５０２は、ＲＡＭ領域２５０３に認証結果識別子が存在するかどうかを確認する。

【０１０９】また、図２６は、認証モジュール１０１がＩＣカードである場合における、認証結果識別子の別の実現方法を示す。符号２６０１、２６０２が付された矩形はデディケーティッドファイル（ＤＦ）を表している。各ＤＦは各カードアプリケーションに対応している。このため、ＤＦがセレクトされると対応するカードアプリケーションが起動する。以後においては、符号２６０１のＤＦは、カードアプリケーションＡに対応し、

同様に符号２６０２のＤＦは、アプリケーションＢに対応しているとする。符号２６０３、２６０４、２６０５、２６０６、２６０７が付された矩形は、エレメンタリファイル（ＥＦ）を表している。ＤＦに対応するカードアプリケーションが起動すると、それに対応するＤＦの直下のＥＦが操作できるようになっている。例えば、符号２６０１のＤＦがセレクトされ、カードアプリケーションＡが起動すると、カードアプリケーションＡは、符号２６０３、２６０４のＥＦをアクセスすることができるようになる。

【０１１０】以降では、カードアプリケーションＡがＴＲＭアクセスライブラリ部４０１を認証し、正しく認証された場合に、符号２６０４のＥＦに認証結果識別子をセットすると仮定する。符号２６０４が付されたＥＦの状態を符号２６０１が付されたＤＦのセキュリティステイタスに含めることにより、ＤＦとＥＦとが形成する木構造における符号２６０１が付されたＤＦの子孫に相当するＤＦのセレクトを制御することができる。つまり、符号２６０２のＤＦのセレクトは、符号２６０１が付されたＤＦの子孫のいずれか、ここでは、符号２６０４が付されたＥＦ内の識別子の存在を条件とする設定をする。すなわち、カードアプリケーションＡによるＴＲＭアクセスライブラリ部４０１の認証の結果により、カードアプリケーションＢに対応するＤＦのセレクトを制御することができるようになるので、カードアプリケーションＢをＴＲＭアクセスライブラリ部４０１が認証された場合にのみ起動させることができるようになる。

【０１１１】このような実施の形態により、ＴＲＭアクセスライブラリ部４０１が認証モジュール１０１によって認証されない限り、認証モジュール内アプリケーション２１０４は端末アプリケーション２１０２からアクセスされることがないので、認証モジュール１０１のセキュリティが保たれる。

【０１１２】なお、認証モジュール内アプリケーション保持部２１０３は、ＴＲＭ部１０３の外部にあってもよい。その場合、認証モジュール内アプリケーション２１０４は、ＴＲＭアクセスライブラリ部認証部４０２によるＴＲＭアクセスライブラリ部４０１が認証されているかどうかを調べて端末アプリケーション２１０２のアクセスを受け入れて動作することになる。

【０１１３】（実施の形態１０）図２７は、本発明の実施の形態１０に関するアプリケーション認証システムの機能ブロック図を示す。本発明の実施の形態１０では、認証モジュール内アプリケーションは、端末で動作するアプリケーションの認証を条件として、そのアプリケーションからのアクセスを受け入れて動作する。図２７は、本実施の形態におけるアプリケーション認証システムの機能ブロック図を示す。本実施の形態におけるアプリケーション認証システムにおいては、実施の形態９におけるアプリケーション認証システムのＴＲＭ部１０３

が、アプリ認証結果識別子生成手段２７０１を有している形態になっている。

【０１１４】アプリ認証結果識別子生成手段２７０１は、ＴＲＭアクセスライブラリ部４０１によるアプリケーションの認証の成功を条件としてアプリ認証結果識別子２７０２を生成する。ここに、「アプリケーション」とは、ダウンロード部１０２にダウンロードされたアプリケーションである。「ＴＲＭアクセスライブラリ部４０１によるアプリケーションの認証」とは、アプリケーションに付された署名と、ＴＲＭアクセスライブラリ部４０１が生成した署名認証用ダイジェストに基づいて行なわれる認証を意味する。

【０１１５】本実施の形態において、認証モジュール内アプリケーション２１０４は、認証の成功を示すアプリ認証結果識別子の存在を条件として、端末アプリケーションに対して認証モジュール内アプリケーション２１０４に対するアクセスを可能とし、認証モジュール内アプリケーション２１０４は端末アプリケーションからのアクセスを受け入れる。

【０１１６】例えば、最初に端末アプリケーション２１０２が動作をしており、それに対して、認証モジュール内アプリケーションがまだ動作をしていない場合、認証モジュール内アプリケーションを起動する際には、アプリ認証結果識別子２７０２の存在する場合に限り、認証モジュール内アプリケーションが起動される。あるいは、端末アプリケーション２１０２と認証モジュール内アプリケーション２１０４との両方が起動している場合には、端末アプリケーション２１０２から認証モジュール内アプリケーション２１０４へアクセスが発生した場合には、アプリ認証結果識別子２７０２の存在する場合に限り、そのアクセスを受け入れる。

【０１１７】端末１００内で認証モジュール内アプリケーションにアクセスする端末アプリケーションが１つだけ動作するのであれば、アプリ認証結果識別子２７０２は一種類あれば十分である。しかし、そのような端末アプリケーションが複数個、端末１００内で動作するのであれば、どの端末アプリケーションが認証されたかを示すために、端末アプリケーション別にアプリ認証結果識別子がアプリ認証結果識別子生成手段２７０１により生成されることになる。あるいは、２個以上の端末アプリケーションが同時に認証モジュール内アプリケーションにアクセスすることがないと保証される場合には、アプリ認証識別子は一種類だけ生成されることとし、認証された端末アプリケーションが認証モジュール内アプリケーションにアクセスする瞬間だけ、そのアプリ認証識別子が生成され、認証された端末アプリケーションによる認証モジュール内アプリケーションのアクセスが終了すると、そのアプリ認証識別子を削除するようにしてもよい。

【０１１８】このような実施の形態により、認証を受け

た端末アプリケーションのみが認証モジュール内アプリケーションにアクセスすることができ、認証モジュール１０１のセキュリティが確保される。

【０１１９】（実施の形態１１）図２８は、本発明の実施の形態１１にかかわるアプリケーション認証システムの機能ブロック図を示す。本実施の形態におけるアプリケーション認証システムは、端末と、認証モジュールと、アプリケーションを端末にダウンロードするサーバと、からなる。

【０１２０】図２８において、端末２８０１は、ダウンロード部２８０４を有する。ダウンロード部２８０４は、アプリケーションをダウンロードする部である。例えば、サーバ２８０３よりアプリケーションをダウンロードする。

【０１２１】認証モジュール２８０２は、ＴＲＭ部２８０５を有する。ＴＲＭ部２８０５は、アプリケーションの認証の処理のための情報を耐タンパ領域に保持する。ここで、「アプリケーション」とは、端末２８０１のダウンロード部２８０４にダウンロードされたアプリケーションを意味する。「アプリケーションの認証」とは、アプリケーションが、信頼のおける者によって発行されたかどうか、不正な動作をしないことの保証を受けているものであるかどうか、あるいは、信頼のおける者から発行されてからの改ざん又は不正な動作をしないことが保証されてからの改ざんがされていないかどうか、などアプリケーションが不正な動作をしないことを確認することである。この処理の方法としては、通常、ＳＨＡ－１やＭＤ５などの、入力データを処理して得られる結果データが一致するような二つの異なる入力データを見つけることが困難なハッシュ関数を用いて、アプリケーションの実行のためのデータを入力データとして処理して得られる結果データを求め、それを暗号化したもの（いわゆる「署名」）が用いられる。従って「アプリケーションの認証の処理のための情報」とは、この署名そのもの、あるいは、署名を復号してハッシュ値を得るのに必要な復号鍵である。「耐タンパ領域」とは、認証モジュールの記憶領域であって、その記憶領域のデータを不正に読み出すことや、その記憶領域のデータを不正に書き換えることが困難な記憶領域である。例えば、その記憶領域にアクセスするためには、正しい手順を行なわないとアクセスできないハードウェアを経由しなければならないようにしたり、記憶領域に記憶されているデータが暗号化されているようにしたりする。

【０１２２】サーバ２８０３は、端末認証部２８０６を有する。端末認証部２８０６は、端末２８０１を介した認証モジュール２８０２の認証が成功することを条件に端末２８０１の認証が成功したと判断する。すなわち、サーバ２８０３は、認証モジュール２８０２を認証することを行なう。その際、サーバ２８０３と認証モジュール２８０２とは通信を行なう必要があるが、その通信

は、端末２８０１を中継して行なわれる。サーバ２８０３が認証モジュール２８０２の認証を行なう方法としては、サーバ２８０３は、乱数を発生し、その乱数を認証モジュールの公開鍵によって暗号化を行い、端末２８０１を介して認証モジュール２８０２へ、暗号化された乱数を復号するように要求する。認証モジュール２８０２は、耐タンパ領域に格納されている認証モジュール２８０２の秘密鍵を用いた復号によりサーバ２８０３が発生した乱数を取得し、それを端末２８０１の中継によりサーバ２８０３へ返す。サーバ２８０３は、発生した乱数と、認証モジュール２８０２から送られてきた乱数が等しいかどうかを判断して認証を行なう。あるいは、サーバ２８０３は、乱数をそのまま認証モジュール２８０２へ送り、認証モジュール２８０２は、秘密鍵によって暗号化を行い、その結果をサーバ２８０３へ返し、サーバ２８０３は、認証モジュール２８０２の公開鍵によって復号を行い、認証モジュール２８０２へ送った乱数と等しいかどうかで認証モジュールを認証する方法もある。

【０１２３】認証モジュール２８０２は端末２８０１に装着されるものであるので、サーバ２８０３が認証モジュール２８０２を認証することにより、認証モジュール２８０２が装着された端末２８０１も認証されることとなる。また、端末２８０１の持つ固有な情報、例えば、端末２８０１の製造番号や、機器の種別を示す識別子、端末２８０１のＲＯＭに格納された識別子、バージョン番号が認証モジュールの耐タンパ領域に存在することを条件として認証モジュール２８０２が端末２８０１を認証することにすれば、認証がより確かなものとなる。

【０１２４】これにより、サーバ２８０３は、端末２８０１に耐タンパ領域が無くても端末２８０１を認証することが可能となり、サーバ２８０３は、端末２８０１を正しく認証することができ、サーバ２８０３と端末２８０１の間で課金処理、決済処理などが行なえる。また、サーバ２８０３から端末２８０１へ機密性の高いデータを含むアプリケーションをダウンロードすることが可能となり、複雑な商取引操作が本実施の形態におけるアプリケーション認証システムにおいて実行することが可能となる。

【０１２５】（実施の形態１２）図２９は、本発明の実施の形態１２に関するアプリケーション認証システムの機能ブロック図を示す。本実施の形態においては、アプリケーション認証システムは、実施の形態１１のように端末２８０１、認証モジュール２８０２、アプリケーションを端末２８０１にダウンロードするサーバ２８０３と、からなる。

【０１２６】端末２８０１は、ダウンロード部２８０４とＴＲＭアクセスライブラリ部２９０１とを有している。ダウンロード部２８０４は、アプリケーションをダウンロードする。この場合、アプリケーションは、サーバ２８０３よりダウンロードされる。あるいは、サーバ

２８０３以外よりダウンロードされてもよい。ＴＲＭアクセスライブラリ部２９０１は、認証モジュール２８０２に自身が認証されることを条件としてアプリケーションの認証のための処理をする。すなわち、ＴＲＭアクセスライブラリ部２９０１は、認証モジュール２８０２に自身を認証させ、正しく認証が行なわれると、ダウンロード部２８０４にダウンロードされたアプリケーションの認証のための処理を行なう。ＴＲＭアクセスライブラリ部２９０１が、認証モジュール２８０２に自身を認証させる方法としては、端末２８０１の固有な情報、例えば、製造番号や、種類を示す識別子、あるいは、ＴＲＭアクセスライブラリ部２９０１を実現するソフトウェアのシリアル番号、バージョン番号などを認証モジュール２８０２に出力し、認証モジュール２８０２の耐タンパ領域に出力された端末２８０１の固有な情報やシリアル番号、バージョン番号などが存在するかどうかで行なう方法がある。

【０１２７】認証モジュール２８０２は、ＴＲＭ部２８０５と、ＴＲＭアクセスライブラリ部認証部２９０２とを有する。ＴＲＭ部２８０５は、ＴＲＭアクセスライブラリ部２９０１を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持する。「ＴＲＭアクセスライブラリ部認証情報」としては上述のように、端末２８０１の固有な情報、例えば、製造番号や、種類を示す識別子、あるいは、ＴＲＭアクセスライブラリ部２９０１を実現するソフトウェアのシリアル番号、バージョン番号などが挙げられる。ＴＲＭアクセスライブラリ部認証部２９０２は、ＴＲＭアクセスライブラリ部認証情報に基づいて端末２８０１のＴＲＭアクセスライブラリ部２９０１を認証する。この認証の方法としては、上述のように、ＴＲＭアクセスライブラリ部２９０１より出力された端末２８０１の固有な情報やＴＲＭアクセスライブラリ部のシリアル番号、バージョン番号などの識別情報をＴＲＭアクセスライブラリ部認証部２９０２が受け取り、ＴＲＭ部２８０５にその識別情報が存在するかどうかで行なう方法がある。この認証の結果は、ＴＲＭアクセスライブラリ部認証部２９０２よりＴＲＭアクセスライブラリ部２９０１へ出力される。また、この認証の結果は、認証モジュール２８０２内に保持され、その後の端末との情報の交換の際に参照され、ＴＲＭアクセスライブラリ部２９０１が正しく認証されていれば、認証モジュール２８０２は正しい情報の交換を行い、そうでなければ、正しくない情報の交換を行なうようにする。

【０１２８】サーバ２８０３は、サーバＴＲＭアクセスライブラリ部認証部２９０３を有する。サーバＴＲＭアクセスライブラリ部認証部２９０３は、端末２８０１のアクセスライブラリ部２９０１を介する認証モジュール２８０２のＴＲＭ部２８０５の認証が成功することを条件としてＴＲＭアクセスライブラリ部２９０１の認証が成功したと判断する。サーバＴＲＭアクセスライブラリ部認証部２９０３が、端末２８０１のアクセスライブラリ部２９０１を介する認証モジュール２８０２のＴＲＭ部２８０５の認証を行なう方法としては、次のものがある。すなわち、サーバ２８０３は、乱数を発生し、その乱数を認証モジュール２８０２の公開鍵によって暗号化を行い、端末２８０１を介して認証モジュール２８０２へ、暗号化された乱数を復号するように要求する。認証モジュール２８０２は、耐タンパ領域に格納されている自身の秘密鍵を用いて、乱数を復号し、それを端末２８０１を介してサーバ２８０３へ返す。サーバ２８０３は、発生した乱数と、認証モジュール２８０２から送られてきた乱数が等しいかどうかを判断して認証を行なう。あるいは、サーバ２８０３は、乱数をそのまま認証モジュール２８０２へ送り、認証モジュール２８０２は、自身の秘密鍵によって暗号化を行い、その結果をサーバ２８０３へ返し、サーバ２８０３は、認証モジュール２８０２の公開鍵によって復号を行い、認証モジュール２８０２へ送った乱数と等しいかどうかで認証モジュールを認証する方法もある。

【０１２９】図３０は、サーバＴＲＭアクセスライブラリ部認証部２９０３と、ＴＲＭアクセスライブラリ部２９０１と、認証モジュール２８０２との相互作用を説明するシーケンス図である。ステップＳ３００１において、ＴＲＭアクセスライブラリ部２９０１より、自身を認証する要求が認証モジュール２８０２へ出力され、ステップＳ３００２において、認証モジュールでの認証結果が出力される。ステップＳ３００３において、サーバＴＲＭアクセスライブラリ部認証部２９０３よりＴＲＭアクセスライブラリ部２９０１へ認証要求が出力され、これに対応して、ステップＳ３００４において、認証要求がＴＲＭアクセスライブラリ部２９０１より認証モジュール２８０２へ出力され、ステップＳ３００５において、認証モジュールは、自身がサーバＴＲＭアクセスライブラリ部認証部２９０３へ認証されるように結果を返す。この際、ＴＲＭアクセスライブラリ部２９０１が正しく認証されているかどうかによって、正しい結果を返したり、正しくない結果を返したりする。ステップＳ３００６において、ＴＲＭアクセスライブラリ部２９０１は、サーバＴＲＭアクセスライブラリ部認証部２９０３へ、認証モジュール２８０２から出力された結果を返す。サーバＴＲＭアクセスライブラリ部認証部２９０３は、この結果を調べ、認証モジュール２８０２が認証できれば、ＴＲＭアクセスライブラリ部２９０１も認証されたものと判断することになる。

【０１３０】上述のように、ＴＲＭアクセスライブラリ部２９０１のＴＲＭアクセスライブラリ部認証部２９０２による認証の結果は認証モジュール２８０２内に保持され、その認証の結果に応じて、認証モジュール２８０２は正しい情報の交換を行なったり、行なわなかったり

するので、サーバ２８０３がＴＲＭアクセスライブラリ部２９０１を介して認証モジュールのＴＲＭ部の認証を行い、正しく認証ができれば、ＴＲＭアクセスライブラリ部２９０１の認証が成功したと判断してよいことになる。

【０１３１】これにより、サーバ２８０３は、端末２８０１に耐タンパ領域が無くても端末２８０１を認証することが可能となり、サーバ２８０３は、端末２８０１を正しく認証することができ、サーバ２８０３と端末２８０１の間で課金処理、決済処理などが行なえる。また、サーバ２８０３から端末２８０１へ機密性の高いデータを含むアプリケーションをダウンロードすることが可能となり、複雑な商取引操作が本実施の形態におけるアプリケーション認証システムにおいて実行することが可能となる。

【０１３２】また、ＴＲＭアクセスライブラリ部２９０１がＴＲＭアクセスライブラリ部認証部２９０２により認証されると、ＴＲＭアクセスライブラリ部２９０１は、認証モジュールにより信頼できるものと判断される。これにより、ダウンロード部２８０４にダウンロードされたアプリケーションの認証の処理の全部または一部をＴＲＭアクセスライブラリ部２９０１に行なうようにすると、ＴＲＭアクセスライブラリ部２９０１によるアプリケーションの認証の処理の全部または一部の結果は認証モジュール２８０２にとって信頼できるものとなる。したがって、ＴＲＭアクセスライブラリ部２９０１によるアプリケーションの認証の処理の全部または一部の結果を用いて、認証モジュール２８０２はダウンロード部２８０４にダウンロードされたアプリケーションの認証を行なうことが可能となる。この結果、正しく認証されたアプリケーションに、認証モジュール内のデータのアクセスを許可することができ、複雑な商取引の操作を行なうことができるようになる。

【０１３３】なお、ＴＲＭアクセスライブラリ部２９０１によるアプリケーションの認証のための処理は、アプリケーションが認証モジュール２８０２のＴＲＭ部２８０５の耐タンパ領域へアクセスしたことを条件に行なうようにしてもよい。これにより、耐タンパ領域にアクセスしないアプリケーションの認証を行なう必要がなくなる。

【０１３４】また、ＴＲＭアクセスライブラリ部２９０１は、アプリケーションの認証のための処理を、アプリケーションがダウンロード部２８０４にダウンロードされたことを条件に行なうようにしてもよい。これにより、ダウンロードされたアプリケーションが全て認証され、不正なアプリケーションが端末２８０１で実行される虞がなくなる。

【０１３５】また、ＴＲＭアクセスライブラリ部２９０１は、アプリケーション認証のための処理を、アプリケーションの実行の開始をトリガとして行なうようにしてもよい。これにより、ダウンロードされたが、実行されないアプリケーションの認証を省略することができる。

【０１３６】（実施の形態１３）図３１は、本発明の実施の形態１３に関するアプリケーション認証システムの機能ブロック図を示す。本実施の形態に関するアプリケーション認証システムは、端末２８０１と、認証モジュール２８０２と、アプリケーションを端末２８０１にダウンロードするサーバ２８０３とからなる。

【０１３７】端末２８０１は、ダウンロード部２８０４と、ＴＲＭアクセスライブラリ部２９０１と、を有し、ＴＲＭアクセスライブラリ部２９０１は、署名用ダイジェスト生成手段３１０１と、ダウンロードアプリケーション署名取得手段３１０２と、アプリ認証データ出力手段３１０３とを備えている。

【０１３８】ダウンロード部２８０４は、アプリケーション３１０４をダウンロードする。アプリケーション３１０４は、サーバ２８０３よりダウンロードされてもよい。また、サーバ２８０３以外、例えば、認証モジュール２８０２からダウンロードされてもよい。本実施の形態においてはアプリケーション３１０４は、アプリケーション３１０４の署名３１０５と共にダウンロードされるものとする。「署名３１０５と共にダウンロードされる」とは、同時にダウンロードされるということのみならず、アプリケーション３１０４のダウンロードと署名３１０５のダウンロードとは前後して行なわれてもよく、後述のアプリケーション３１０４の認証が行なわれる時までには、アプリケーション３１０と署名３１０５とがダウンロードされていることを意味する。

【０１３９】署名用ダイジェスト生成手段３１０１は、アプリケーションから署名用ダイジェストを生成する。すなわち、ダウンロード部２８０４にダウンロードされたアプリケーション３１０４から署名用ダイジェストを生成する。「署名用ダイジェスト」とは、署名３１０５を生成するときに使われたハッシュ関数と同じハッシュ関数を用いて得られる値である。

【０１４０】ダウンロードアプリケーション署名取得手段３１０２は、アプリケーション３１０４のダウンロードと共にダウンロードされた署名３１０５を取得する。上述のように「アプリケーション３１０４のダウンロードと共にダウンロードされた」とは、同時にダウンロードされたということのみならず、後述のアプリケーション３１０４の認証が行なわれる時までには、アプリケーション３１０４と署名３１０５とのダウンロードが終了していることを意味する。

【０１４１】アプリ認証データ出力手段は、取得した署名と、署名用ダイジェスト生成手段３１０１とによって生成された署名用ダイジェストと、をサーバに送信する。「取得した署名」とは、ダウンロードアプリケーション署名取得手段３１０２により取得された署名３１０５である。

【０１４２】署名用ダイジェスト生成手段３１０１と、ダウンロードアプリケーション署名取得手段３１０２と、アプリ認証データ出力手段３１０３とは、ダウンロード部２８０４にダウンロードされたアプリケーション３１０４を認証するための処理を行なう。この処理は、ＴＲＭアクセスライブラリ部２９０１が認証モジュール２８０２により認証されたことを条件として行なわれるようにしてもよい。

【０１４３】認証モジュールは、ＴＲＭ部２８０５とＴＲＭアクセスライブラリ部認証部２９０２と、を有している。ＴＲＭ部２８０５とＴＲＭアクセスライブラリ部認証部２９０２とは、実施の形態１２のＴＲＭ部とＴＲＭアクセスライブラリ部と同じものである。

【０１４４】サーバ２８０３は、サーバＴＲＭアクセスライブラリ部認証部２９０３と、アプリ認証データ入力部３１０６と、サーバアプリ認証部３１０７とを有する。

【０１４５】サーバＴＲＭアクセスライブラリ部認証部２９０３は、実施の形態１２におけるものと同じであり、端末２８０１のＴＲＭアクセスライブラリ部２９０１を介する認証モジュールのＴＲＭ部２８０５の認証が成功することを条件としてＴＲＭアクセスライブラリ部２９０１の認証が成功したと判断する。

【０１４６】アプリ認証データ入力部３１０６は、サーバＴＲＭアクセスライブラリ部認証部２９０３により認証が成功したと判断されたＴＲＭアクセスライブラリ部２９０１のアプリ認証データ出力手段３１０３から出力された署名用ダイジェストと、署名と、を入力する。

【０１４７】サーバアプリ認証部３１０７は、アプリ認証データ入力部３１０６に入力された署名用ダイジェストと、署名と、に基づいてアプリケーションの認証を行なう。認証は、署名を復号してダイジェストを求め、そのダイジェストが署名用ダイジェストと等しいかどうかを判断することにより行なわれる。もし、署名が公開鍵暗号化方式のサーバ２８０３の秘密鍵で暗号化されている場合には、アプリ認証データ入力部３１０６に入力された署名用ダイジェストをサーバ２８０３の秘密鍵で暗号化し、得られたものがアプリ認証データ入力部３１０６に入力された署名と等しいかどうかで判断するようにしてもよい。

【０１４８】図３２は、本実施の形態におけるアプリケーション認証システムを構成するサーバ２８０３、端末２８０１、認証モジュール２８０２の時間に沿った相互作用を示す。ステップＳ３２０１からステップＳ３２０６までは、実施の形態１２における図３０におけるステップＳ３００１からステップＳ３００６までと同じである。ステップＳ３２０６の後、アプリケーション３１０４がダウンロード部２８０４にダウンロードされると、署名用ダイジェスト生成手段３１０１により、アプリケーション３１０４の署名用ダイジェストが生成され、ダ

ウンロードアプリケーション署名取得手段３１０２により、署名３１０５が取得され、アプリ認証データ出力手段３１０３により、アプリ認証データ入力部３１０６へ署名用ダイジェストと署名が入力される（ステップＳ３２０７）。その後、サーバアプリ認証部３１０７によりアプリ認証データ入力部３１０６へ入力された署名用ダイジェストと署名によりアプリケーション３１０４の認証が行なわれる。

【０１４９】本実施の形態によれば、サーバ２８０３のサーバＴＲＭアクセスライブラリ部認証部２９０３が、端末２８０１のＴＲＭアクセスライブラリ部２９０１を介する認証モジュール２８０２のＴＲＭ部２８０５の認証が成功することを条件として端末２８０１のＴＲＭアクセスライブラリ部２９０１の認証が成功したと判断する。このため、サーバ２８０３は、ＴＲＭアクセスライブラリ部２９０１のアプリ認証データ出力手段３１０３がアプリ認証データ入力部３１０６へ送信するアプリケーション３１０４の署名用ダイジェストと署名３１０５が、実際にアプリケーション３１０４に由来するものであると判断することができ、サーバは、アプリケーション３１０４を認証することができる。

【０１５０】（実施の形態１４）図３３は、本発明の実施の形態１４に関するアプリケーション認証システムの機能ブロック図を示す。本実施の形態１３においては、ダウンロード部２８０４にダウンロードされたアプリケーションの認証の処理の一部がサーバ２８０３で実行されるようになっていたが、本実施の形態においては、サーバ２８０３以外でアプリケーションの認証が行なわれ、サーバ２８０３は認証の結果だけを取得するようになっている。

【０１５１】端末２８０１は、ダウンロード部２８０４とＴＲＭアクセスライブラリ部２９０１とを有している。ダウンロード部２８０４は、アプリケーションをダウンロードする。ＴＲＭアクセスライブラリ部２９０１は、認証成功情報生成手段３３０１と認証成功情報出力手段３３０３とを備えている。

【０１５２】認証成功情報生成手段３３０１は、アプリケーションの認証の成功を示す認証成功情報３３０２を生成する。本実施の形態において、アプリケーションの認証は、ＴＲＭアクセスライブラリ部２９０１内のみで行なわれるようになっていてもよい。また、ＴＲＭアクセスライブラリ部２９０１と認証モジュール２８０２とが協働して行なうようになっていてもよく、認証成功情報生成手段３３０１は、その認証の結果を取得し、認証が成功したかどうかを示す認証成功情報３３０２を生成する。このとき、認証成功情報３３０２を認証モジュール２８０２の秘密鍵やサーバ２８０３の公開鍵により認証成功情報３３０２が暗号化されるようにしてもよい。

【０１５３】認証成功情報出力手段３３０３は、認証成功情報生成手段３３０１にて生成された認証成功情報３

３０２を出力する。もし、認証成功情報３３０２が暗号化されていない場合には、認証成功情報３３０２を認証モジュール２８０２の秘密鍵やサーバ２８０３の公開鍵により認証成功情報３３０２を暗号化して出力するようにしてもよい。

【０１５４】認証モジュール２８０２は、ＴＲＭ部２８０５と、ＴＲＭアクセスライブラリ部認証部２９０２と、を有し、実施の形態１３と同じ動作をする。

【０１５５】サーバ２８０３は、サーバＴＲＭアクセスライブラリ部認証部と、認証成功情報入力部３３０４と、サーバアプリ認証部３３０５とを有している。

【０１５６】サーバＴＲＭアクセスライブラリ部認証部は、実施の形態１３と同じ動作をする。

【０１５７】認証成功情報入力部３３０４は、サーバＴＲＭアクセスライブラリ部認証部により認証が成功したと判断されたＴＲＭアクセスライブラリ部の認証成功情報出力手段から出力された認証成功情報を入力する。ＴＲＭアクセスライブラリ部２９０１がサーバＴＲＭアクセスライブラリ部認証部により認証が成功したと判断された場合には、ＴＲＭアクセスライブラリ部２９０１と認証モジュール２８０２とにより出力される情報は、サーバ２８０３にとって信頼のおけるものであるので、認証成功情報出力手段３３０３の内容は、信頼のおけるものと判断することができる。

【０１５８】サーバアプリ認証部３３０５は、認証成功情報入力部３３０４に入力された認証成功情報に基づいてアプリケーションの認証を行なう。例えば、認証成功情報出力手段３３０３により出力された認証成功情報が、認証モジュール２８０２の秘密鍵やサーバ２８０３の公開鍵で暗号化されている場合には、復号を行い、認証成功情報の内容を調べてダウンロード部２８０４にダウンロードされたアプリケーションを認証する。

【０１５９】（実施の形態１５）本発明においては、アプリケーション（アプリケーションプログラム）を認証するために、アプリケーションのダウンロードを行なうと共に、署名をダウンロードすることが必要となる。以下では、アプリケーションの中に、アプリケーションの署名を格納したアプリケーションを説明する。

【０１６０】アプリケーションプログラムは、通常、アプリケーション本体と、アプリケーション定義ファイルに分けることができる。「アプリケーション本体」とは、アプリケーションプログラムを実行するためのコードやデータであり、「アプリケーション定義ファイル」とは、アプリケーション本体の属性を記述するファイルであり、「アプリケーション本体の属性」としては、例えば、アプリケーション本体の大きさ、アプリケーションプログラムを実行するためのエントリポイント、アプリケーションプログラムの実行時にアプリケーションプログラムに渡されるべきパラメータ（Ｊａｖａ（登録商標）においては、メインクラスの起動パラメータ）など

がある。アプリケーション定義ファイルにおいて、アプリケーション本体の属性を記述する部分を「属性情報格納部」と呼ぶことにすると、属性情報格納部に、アプリケーションの作成者が自由に利用できるオプショナル領域が存在する場合がある。そこで、このオプショナル領域に、アプリケーション本体の署名データを格納するようにしてもよい。なお、アプリケーション本体は、コードとデータそのものではなく、コードとデータとを圧縮したものであってもよい。同様に、アプリケーション定義ファイルもアプリケーション本体の属性の記述を圧縮したものであってもよい。

【０１６１】図３４は、Ｊａｖａ（登録商標）アプリケーション、特に、ｉアプリのアプリケーションの構造を例示している。ｉアプリにおいては、アプリケーション本体はＪＡＲファイル３４０１に格納され、アプリケーション定義ファイルは、ＡＤＦファイル３４０２として提供されるようになっている。ＡＤＦファイル３４０２に格納されたアプリケーション本体の属性は、アプリケーションの名前としてＡｐｐＮａｍｅという必須キーにより示され、アプリケーション本体のサイズはＡｐｐＳｉｚｅという必須キーにより示される。さらに、アプリケーションの作成者が自由に利用できるオプショナル領域として、ＡｐｐＰａｒａｍというオプショナルキーで示されるものがある。このＡｐｐＰａｒａｍで示される領域は、最長２５５バイト利用可能である。一方、アプリケーション本体の署名は、１６０ビットの楕円暗号を用いると２０バイト必要であり、１０２４ビットのＲＳＡ暗号を用いるのであれば、１２８バイト必要であり、ＡｐｐＰａｒａｍで示される領域に収まることになる。よってアプリケーション本体の署名をＡｐｐＰａｒａｍで示される領域に格納することが可能となる。

【０１６２】図３５は、このように、オプショナル領域にアプリケーション本体の署名データを格納したアプリケーションを認証する場合の動作を説明するフローチャートである。ステップＳ３５０１において、オプショナル領域から署名データを取得する。ステップＳ３５０２において、ステップＳ３５０１で取得された署名データを利用して、署名を検証することを行なう。これらのステップは、プログラムによって実行可能である。

【０１６３】また、図３４は、アプリケーションプログラムのデータ構造を示しているとみなすこともできる。すなわち、コード及びデータの圧縮ファイルであるＪＡＲファイルを格納するＪＡＲファイル部３４０１とアプリケーションの定義ファイルであるＡＤＦファイルを格納するＡＤＦファイル部３４０２とからなるデータ構造とみなすこともできる。このようなデータ構造において、ＡＤＦファイル部３４０２のＡＤＦファイルには、メインクラスの起動パラメータなどを格納するＡｐｐＰａｒａｍで示される領域があり、ＡｐｐＰａｒａｍで示される領域に、ＪＡＲファイル部３４０１に格納されて

いるＪＡＲファイルの署名が格納されている。

【０１６４】ＡｐｐＰａｒａｍで示される領域に格納されるＪＡＲファイルの署名は、アプリケーションの動作を保証する者による署名であってもよい。ここに、「アプリケーションの動作を保証する者」とは、ＪＡＲファイルに格納されたコードとデータにより動作するアプリケーションを作成した者、そのアプリケーションを配布する者、そのアプリケーションの作成した者、そのアプリケーションの動作を検証し不正な動作をしないことを保証する第三者などである。

【０１６５】図３４に示したアプリケーションプログラムのデータ構造は、ビット列（ビットストリーム）によって表現可能であるので、このようなビット列を記録した（ＳＤ）メモリカードや、フロッピー（登録商標）ディスク、コンパクトディスクなどの記録媒体を作成することができる。

【０１６６】このようなアプリケーションプログラムにより、アプリケーションをダウンロードするとアプリケーション本体のみならず、アプリケーション本体の署名もダウンロードされることになり、別に署名をダウンロードする手間を省くことができる。

【０１６７】（実施の形態１６）図３７は、本発明の実施の形態１６に関する端末の機能ブロック図を例示する。本実施の形態の特徴は、実施の形態１のアプリケーション認証システムにおける端末の内部に認証モジュールを備えるようにし、一体化したことである。

【０１６８】本実施の形態において、端末３７００は、ダウンロード部３７０１と、ＴＲＭ部３７０２とを有する。

【０１６９】ダウンロード部３７０１は、アプリケーションをダウンロードする。すなわち、実施の形態１におけるダウンロード部１０２と同じ機能を有する。

【０１７０】ＴＲＭ部３７０２は、アプリケーションの認証のための情報を耐タンパ領域に保持する。すなわち、実施の形態１における認証モジュール１０１内のＴＲＭ部１０３と同じ機能を有する。

【０１７１】したがって、本実施の形態の端末においては、アプリケーションのダウンロードの手順や、ダウンロードされたアプリケーションの認証の手順は、実施の形態１におけるものと同じであってよい。

【０１７２】このような端末を用いることにより、例えば、サービス提供会社から端末３７００のダウンロード部３７０１にダウンロードされたアプリケーションに対して認証の処理を行い、その認証の処理が成功した場合に、アプリケーションに対して、ＴＲＭ部３７０２の保持された情報などの端末に格納された情報へのアクセスを安全に許可することが可能となる。

【０１７３】なお、「端末」という語を用いたが、これは、携帯電話に代表される携帯可能な端末などに限定されることを意味しない。例えば、家庭用電化製品であってもよいし、いわゆる、情報家電やネット家電と呼ばれるものであってもよい。そのような製品を例示列挙すれば、エアコンディショナ、加湿器、除湿器、空気清浄機、電子レンジ、オーブン、冷蔵庫、食器洗い機、湯沸し器、アイロン、ズボンプレッサー、電気掃除機、洗濯機、乾燥機、電気毛布、電気敷布、照明機器、テレビ受像機、ラジオ受信機、テープレコーダなどのオーディオ機器、カメラ、ＩＣレコーダ、電話機、ファクシミリ送受信機、コピー機、プリンター、スキャナー、パーソナルコンピュータ、などを挙げることができる（このことは、次に説明する実施の形態１７における、「端末」についても言える）。

【０１７４】（実施の形態１７）図３８は、本発明の実施の形態１７に関する端末の機能ブロック図を例示する。本実施の形態の特徴は、実施の形態２などのアプリケーション認証システムにおける端末の内部に認証モジュールを備えるようにして、端末と認証モジュールとを一体化したことである。

【０１７５】本実施の形態において、端末３８００は、認証モジュール３８０１を備えた端末となっており、ダウンロード部３８０２と、ＴＲＭアクセスライブラリ部３８０３と、を有している。認証モジュール３８０１は、ＴＲＭ部３８０４と、ＴＲＭアクセスライブラリ部認証部３８０５と、を有している。

【０１７６】認証モジュール３８０１は、耐タンパ領域に情報を保持しその情報を用いて認証のための処理を行なう。詳細については、後述する。

【０１７７】ダウンロード部３８０２は、アプリケーションをダウンロードする。すなわち、実施の形態２などにおけるダウンロード部１０２と同じ機能を有する。

【０１７８】ＴＲＭアクセスライブラリ部３８０３は、認証モジュール３８０１に自身が認証されることを条件としてアプリケーションの認証のための処理をする。すなわち、実施の形態２などにおけるＴＲＭアクセスライブラリ部４０１と同じ機能を有する。なお、「認証モジュール３８０１に自身が認証される」とは、後述のように、ＴＲＭアクセスライブラリ部認証部３８０５により認証がされることを意味する。

【０１７９】ＴＲＭ部３８０４は、ＴＲＭアクセスライブラリ部認証情報を前記耐タンパ領域に保持する。「ＴＲＭアクセスライブラリ認証情報」とは、ＴＲＭアクセスライブラリ部を認証するための情報であり、実施の形態２の定義と同じである。したがって、ＴＲＭ部３８０４は、実施の形態２などのＴＲＭ部１０３と同じ機能を有する。なお、耐タンパ領域は、ＴＲＭ部３８０４の内部にあってもよいし、認証モジュール３８０１の内部であってＴＲＭ部３８０４の外部にあってもよい。

【０１８０】ＴＲＭアクセスライブラリ部３８０５は、ＴＲＭアクセスライブラリ部認証情報に基づいてＴＲＭアクセスライブラリ部３８０３を認証する。したがっ

て、ＴＲＭアクセスライブラリ部３８０５は、実施の形態２などのＴＲＭアクセスライブラリ部４０２と同じ機能を有する。

【０１８１】図３９は、本実施の形態における端末３８００の処理の流れを説明するフローチャートを例示する。このフローチャートに例示された処理においては、ダウンロード部３８０２にアプリケーションがダウンロードされていることが仮定されている。

【０１８２】ステップＳ３９０１において、ＴＲＭアクセスライブラリ部認証部３８０５により、ＴＲＭアクセスライブラリ部３８０３の認証の処理を行なう。

【０１８３】ステップＳ３９０２において、ＴＲＭアクセスライブラリ部３８０３が認証されたかどうかが判断され、もし認証されたのであれば、ステップＳ３９０３へ処理が進められる。図３９では、もし認証されなければ、処理が終了することになっているが、その代わりに、ダウンロード部３８０２にダウンロードされたアプリケーションの破棄が行なわれるようになっていてもよい。

【０１８４】ステップＳ３９０３において、ダウンロード部３８０２にダウンロードされたアプリケーションの認証の処理を、ＴＲＭアクセスライブラリ部３８０３により行なう。

【０１８５】ステップＳ３９０４において、ダウンロードされたアプリケーションが認証されたのであれば、ステップＳ３９０５へ処理が進められる。もし、認証されなければ、処理が終了する。処理が終了する代わりに、ダウンロード部３８０２にダウンロードされたアプリケーションの破棄が行なわれるようになっていてもよい。

【０１８６】ステップＳ３９０５において、ダウンロードされたアプリケーションによる認証モジュールへのアクセスが許可される。この許可を行なうのは、認証モジュール３８０１である。あるいは、アプリケーションが認証モジュール３８０１へアクセスする場合に、必ず、ＴＲＭアクセスライブラリ部３８０３の機能を利用するのであれば、ＴＲＭアクセスライブラリ部３８０３により認証モジュールへのアクセスが許可されるようになっていてもよい。

【０１８７】なお、実施の形態２において述べたように、ＴＲＭアクセスライブラリ部３８０２は、アプリケーションマネージャ、デバイスドライバなどを備えていてもよい。

【０１８８】本実施の形態によれば、端末の内部に認証モジュールを備えることにより、端末の内部に高度に保護されるべき情報を保持することが可能となり、端末にダウンロードされたアプリケーションの認証を行なうことが可能となる。

【０１８９】（実施の形態１８）本発明の実施の形態１８は、第一の機器と、認証モジュールと、からなるアプリケーション認証システムに関する。本実施の形態にお

いては、認証モジュールが保持する情報を用いて、第一の機器に格納されたアプリケーションが認証される。

【０１９０】図４０は、本実施の形態のアプリケーション認証システムの機能ブロック図を例示している。アプリケーション認証システムは、第一の機器４００１と、認証モジュール４００２と、からなる。第一の機器は、端末に限られることはなく、例えば、パーソナルコンピュータ、ワークステーション、大型計算機、あるいは、サーバ装置であってもよい。また、第一の機器４００１と認証モジュール４００２とは、電気的に直接接続されている必要はなく、また、物理的に接触している必要もない。例えば、無線によって接続されていてもよい。また、インターネットに代表されるネットワークにより接続されていてもよい。特に、そのネットワークは、光ケーブルなどの電気の伝導を使用しない媒体を用いて構築されていてもよい。

【０１９１】第一の機器４００１は、アプリケーション格納部４００３を有している。アプリケーション格納部４００３は、アプリケーションを格納する。アプリケーションとは、第一の機器４００１で動作するプログラムに限られない。第一の機器４００１以外の機器で動作するアプリケーションであってもよい。また、「格納する」とは、アプリケーションを保持することである。保持する時間の長さは問わない。また、保持の目的も問わない。例えば、アプリケーションを第一の機器４００１で動作させるための格納が目的であってもよい。また、アプリケーションを第一の機器４００１にダウンロードし動作させることが目的であってもよい。あるいは、アプリケーションが通信で送られる際に、第一の機器４００１が中継するための一時的な保持が目的であってもよい。あるいは、アプリケーションを第一の機器４００１以外の機器にダウンロードするための保持が目的であってもよい。

【０１９２】認証モジュール４００２は、ＴＲＭ部４００４を有する。ＴＲＭ部４００４は、アプリケーションの認証の処理のための情報を耐タンパ領域に保持する。アプリケーションの認証の処理のための情報としては、例えば、暗号のための秘密鍵やアプリケーションの署名の真正性を確認するための証明書やなどを挙げることができる。ここでいうアプリケーションとは、第一の機器４００１のアプリケーション格納部４００３に格納されるアプリケーションである。したがって、本実施の形態における認証モジュールのＴＲＭ部４００４は、実施の形態１のＴＲＭ部と同じ機能を有するものであってもよい。その場合、アプリケーションの認証の処理の方法などは、実施の形態と同様のものとなる。

【０１９３】本実施の形態のアプリケーション認証システムにより、第一の機器４００１のアプリケーション格納部４００３に格納されているアプリケーションを認証することが可能となるので、例えば、そのアプリケーシ

ョンが不正な動作をすることを防止することができる。

【０１９４】なお、第一の機器４００１は、家庭用電化製品であってもよい。また、いわゆる、情報家電やネット家電と呼ばれるものであってもよい。そのような製品を例示列挙すれば、エアコンディショナ、加湿器、除湿器、空気清浄機、電子レンジ、オーブン、冷蔵庫、食器洗い機、湯沸し器、アイロン、ズボンプレッサー、電気掃除機、洗濯機、乾燥機、電気毛布、電気敷布、照明機器、テレビ受像機、ラジオ受信機、テープレコーダなどのオーディオ機器、カメラ、ＩＣレコーダ、電話機、ファクシミリ送受信機、コピー機、プリンター、スキャナー、パーソナルコンピュータ、などを挙げることができる。

【０１９５】（実施の形態１９）本発明の実施の形態１９も、実施の形態１８と同じように、第一の機器と認証モジュールとからなるアプリケーション認証システムに関する。本実施の形態においては、第一の機器に格納されるアプリケーションの認証が行なわれるときには、第一の機器内でその認証を行なう部分が認証モジュールにより認証がされる。

【０１９６】図４１は、本実施の形態におけるアプリケーション認証システムの機能ブロック図を例示している。アプリケーション認証システムは、第一の機器４１０１と、認証モジュール４１０２と、からなる。なお、実施の形態１８におけるように、第一の機器４１０１と認証モジュール４１０２とは、電気的に直接接続されている必要もなく、また、物理的に接触している必要もない。

【０１９７】第一の機器４１０１は、アプリケーション格納部４１０３と、ＴＲＭアクセスライブラリ部４１０４と、を有している。

【０１９８】アプリケーション格納部４１０３は、アプリケーションを格納する。例えば、実施の形態１８におけるアプリケーション格納部４００３と同じ機能を有している。

【０１９９】ＴＲＭアクセスライブラリ部４１０４は、認証モジュール４１０２に自身が認証されることを条件としてアプリケーションの認証のための処理をする。ここに「自身」とは、ＴＲＭアクセスライブラリ部４１０４を意味する。あるいは、「自身」とは、ＴＲＭアクセスライブラリ部４１０４を含む部分であってもよい。例えば、第一の機器４１０１自体が「自身」であるとしてもよい。

【０２００】また、「アプリケーション」とは、アプリケーション格納部４００３に格納されたアプリケーションを意味する。

【０２０１】したがって、ＴＲＭアクセスライブラリ部４１０４は、自身を認証モジュールによって認証される処理が行なわれ、その処理の結果、正しく認証された場合に、アプリケーション格納部４１０３に格納されたアプリケーションの認証の処理を行なう。

【０２０２】なお、ＴＲＭアクセスライブラリ部４１０４は、実施の形態２において説明したように、アプリケーションマネージャとデバイスドライバを備え、それらの処理を行なうようになっていてもよい。

【０２０３】認証モジュール４１０２は、ＴＲＭ部４１０５と、ＴＲＭアクセスライブラリ部認証部４１０６と、を有している。

【０２０４】ＴＲＭ部４１０５は、ＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持する。「ＴＲＭアクセスライブラリ部認証情報」とは、ＴＲＭアクセスライブラリ部を認証するための情報である。例えば、第一の機器を特定するための情報を挙げることができる。このような情報としては、第一の機器の製造者番号と製造番号、第一の機器に電話番号が割り振られている場合には、その電話番号を例としてあげることができる。また、第一の機器が接続されている他の機器の情報や第一の機器に装備されている部品を特定する情報、あるいは、第一の機器にインストールされているプログラムのバージョン番号など、第一の機器の置かれている状況を示すものであってもよい。また、第一の機器が、なんらかの秘密の情報、例えば、暗号鍵など、を保持できる場合には、その暗号鍵が真正なことを検出するための情報をＴＲＭアクセスライブラリ部認証情報としてもよい。

【０２０５】また、耐タンパ領域については、実施の形態２の説明を参照されたい。

【０２０６】ＴＲＭアクセスライブラリ部認証部４１０６は、ＴＲＭアクセスライブラリ部認証情報に基づいて第一の機器４１０１のＴＲＭアクセスライブラリ部４１０４を認証する。すなわち、ＴＲＭアクセスライブラリ部４１０４から送られてくる情報を取得し、ＴＲＭアクセスライブラリ部４１０４から得られる情報が、ＴＲＭアクセスライブラリ部認証情報に適合するものであるかどうかを判断し、認証の処理を行なう。

【０２０７】なお、ＴＲＭアクセスライブラリ部認証部４１０６が認証する対象は、ＴＲＭアクセスライブラリ部４１０４にのみ限られるものではなく、ＴＲＭアクセスライブラリ部４１０４を含む部分であってもよく、例えば、第一の機器４１０１の全体を認証するようになっていてもよい。この場合には、ＴＲＭアクセスライブラリ部認証情報は、第一の機器４１０１の製造番号などや第一の機器４１０１が置かれている状況などを用いるようになっていてもよい。

【０２０８】図４２は、本実施の形態におけるアプリケーション認証システムの動作を説明するフローチャートを例示する。

【０２０９】ステップＳ４２０１において、ＴＲＭアクセスライブラリ部４１０４の認証の処理を、ＴＲＭアクセスライブラリ部認証部４１０６により行なう。この際、耐タンパ領域に保持されたＴＲＭアクセスライブラ

リ部認証情報が用いられる。

【０２１０】ステップＳ４２０２において、ステップＳ４２０１の処理によりＴＲＭアクセスライブラリ部４１０４が認証されたかどうかを判断する。もし認証されたと判断された場合には、ステップＳ４２０３において、アプリケーション格納部４１０３に格納されたアプリケーションの認証の処理を、ＴＲＭアクセスライブラリ部４１０４により行なう。

【０２１１】本実施の形態においては、認証モジュール４１０２のＴＲＭアクセスライブラリ部認証部４１０６により認証されたＴＲＭアクセスライブラリ部４１０４がアプリケーションの認証を行なう。このため、アプリケーションの認証の結果が、認証モジュール４１０２にとって、信頼できるものとなる。この結果、アプリケーション格納部４１０３に格納されたアプリケーションの実行により、認証モジュールへのアクセスが発生した場合に、認証モジュールはそのアクセスを許可することができる。また、例えば、アプリケーション格納部４１０３が、他の機器へアプリケーションをダウンロードする目的で備えられたものであっても、アプリケーション格納部４１０３からダウンロードされたアプリケーションからの認証モジュールへのアクセスを許可することができる。また、アプリケーションに、認証モジュール４１０２により認証されたことを示す情報を付加することも可能である。これにより、従来の処理よりも複雑な処理を実現することが可能となる。

【０２１２】（実施の形態２０）実施の形態１９などにおいて示されたアプリケーション認証システムは、第一の機器と、認証モジュールと、の２つの主要な機器から構成されていた。しかし、本実施の形態において示されるように、主要な機器の数は、２つに限定されるものではない。

【０２１３】図４３は、主要な機器の数を３とした場合のアプリケーション認証システムの機能ブロック図を例示している。このアプリケーション認証システムは、第１の機器４３０１と、第２の機器４３０２と、第３の機器４３０３と、からなる。すなわち、アプリケーション認証システムは、３つの主要な部分を持つ。なお、これらの３つの主要な部分は直列に接続されているが、実施の形態１８や実施の形態１９で述べたように、電気的に直接接続されていたり、物理的に接触されるようになっていたりする必要はない。また、第１の機器４３０１、第２の機器４３０２、第３の機器４３０３を所有あるいは占有している者が、一人であってもよいし、これら３つの機器が、異なる者により所有あるいは占有されていてもよい。

【０２１４】実施の形態１９などのアプリケーション認証システムとの対応は次の通りである。すなわち、第１の機器４３０１が認証モジュールに相当し、第３の機器４３０３が、端末や実施の形態１９における第一の機器４１０１に相当する。

【０２１５】第１の機器４３０１は、ＴＲＭ部４３０４と、第１認証処理部４３０５と、を有している。

【０２１６】ＴＲＭ部４３０４は、第２の機器を認証するための認証情報を耐タンパ領域に保持する。したがって、実施の形態１９などのＴＲＭ部と同じ機能を有する。ただ、耐タンパ領域に保持される情報が第２の機器を認証するための認証情報となっている点が異なる。なお、耐タンパ領域には、第２の機器を認証するための情報だけではなく、第３の機器を認証するための情報も保持されていてもよい。この認証情報としては、実施の形態１９でのＴＲＭアクセスライブラリ部認証情報と同様に、機器の製造番号や、機器の置かれている状況を示す情報、あるいは、機器が暗号鍵や証明書を保持できる場合には、その暗号鍵や証明書の真正性を検出するための情報を挙げることができる。

【０２１７】第１認証処理部４３０５は、前記認証情報に基づいて第２の機器４３０２を認証する。「前記認証情報」とは、耐タンパ領域に保持された認証情報である。

【０２１８】第２の機器４３０２は、第２認証処理部４３０６を有する。第２認証処理部４３０６は、第１認証処理部に自身が認証されることを条件として第３の機器４３０３を認証する。ここに「自身」とは、第２認証処理部４３０６を含む第２の機器３４０２を意味する。

【０２１９】第２の機器４３０２が第１認証処理部４３０５により認証された場合、第２の機器４３０２は第１の機器４３０１にとって信頼できる機器とみなすことができる。そのため、第１の機器４３０１は、耐タンパ領域に保持される情報へ第２の機器４３０２がアクセスすることを許すことができる。そこで、第２認証処理部４３０６が第３の機器４３０３を認証する場合には、耐タンパ領域に保持された情報を用いることが可能である。そこで、第２認証処理部４３０６が第３の機器４３０３を認証する際には、耐タンパ領域に保持された情報を用いるようにしてもよい。

【０２２０】このように、第２認証処理部４３０６は、第１の機器４３０１へアクセスするためのデバイスドライバの機能を備えていてもよい。

【０２２１】また、第２認証処理部４３０６は、第３の機器４３０３を認証するために必要な情報を、第１の機器や第３の機器とは異なる別の機器より取得するようにしてもよい。この取得の際に、第２認証処理部４３０６は、第２の機器４３０２が第１認証処理部４３０５により認証されていることを示す情報を提示するようにしてもよい。

【０２２２】第３の機器４３０３は、アプリケーション格納部４３０７と、第３認証処理部４３０８と、を有している。アプリケーション格納部４３０７は、アプリケーションを格納する。したがって、実施の形態１９など

におけるアプリケーション格納部と同じ機能を有する。このため、アプリケーションを格納する時間の長さや格納する目的は特に限定されない。

【０２２３】第３認証処理部４３０８は、第２の機器４３０２に自身が認証されることを条件として、前記アプリケーションの認証のための処理をする。「前記アプリケーション」とは、アプリケーション格納部４３０７に格納されているアプリケーションを意味する。また、「自身」とは、第３の機器４３０３を意味する。

【０２２４】第３の機器４３０３が第２認証処理部４３０６により認証された場合、第３の機器４３０３は第１の機器４３０１にとって信頼できる機器とみなすことができる。そのため、第１の機器４３０１は、耐タンパ領域に保持される情報へ第３の機器４３０３がアクセスすることを許すことができる。そこで、第３認証処理部４３０６がアプリケーションを認証する場合には、耐タンパ領域に保持された情報を用いることが可能である。

【０２２５】また、第３認証処理部４３０８は、アプリケーションを認証するために必要な情報を、第１の機器や第２の機器とは異なる別の機器より取得するようにしてもよい。この取得の際に、第３認証処理部４３０８は、第３の機器４３０２が第２認証処理部４３０６により認証されていることを示す情報を提示するようにしてもよい。また、その際、第２の機器４３０２が第一認証処理部４３０５により認証されていることを示す情報を提示してもよい。

【０２２６】図４４は、第１の機器４３０１の動作を説明するフローチャートを例示する。ステップＳ４４０１において、第１認証処理部４３０５はＴＲＭ部４３０４が耐タンパ領域に保持する認証情報を取得する。ステップＳ４４０２において、第２の機器の認証の処理を行ない、ステップＳ４４０３において、認証できたかどうかを判断する。もし、認証できたのであれば、ステップＳ４４０４において、第２の機器へ、認証されたことを伝達する。

【０２２７】図４５は、第２の機器４３０２の動作を説明するフローチャートを例示する。ステップＳ４５０１において、第１認証処理部４３０５により認証されたかどうかを判断する。この判断は、図４４に示されたステップＳ４４０４において、認証されたことが第１の機器４３０１より伝達されたかどうかにより判断される。もし、認証されたのであれば、ステップＳ４５０２において、第３の機器の認証の処理を、第２認証処理部４３０６により行なう。ステップＳ４５０３において、認証できたかどうかを判断する。もし、認証できたのであれば、ステップＳ４５０４において、第３の機器へ認証されたことを伝達する。

【０２２８】図４６は、第３の機器４３０３の動作を説明するフローチャートを例示する。ステップＳ４６０１において、第２認証処理部４３０６により認証されたかどうかを判断する。この判断は、図４５に示されたステップＳ４５０４において、認証されたことが第２の機器４３０２から伝達されたかどうかにより判断される。もし、認証されたのであれば、ステップＳ４６０２において、アプリケーションの認証の処理を行なう。図４６では、ここで処理が終了するが、アプリケーションの認証の処理の結果を、例えば、第１の機器４３０１へ伝達してもよい。また、第２の機器４３０２へ伝達してもよい。また、もし、アプリケーションが他の機器へアクセスする場合には、第３認証処理部４３０８により認証されたことを示す情報を提示するようにしてもよい。あるいは、アプリケーションに第３認証処理部４３０８により認証されたことを示す情報を付加してもよい。

【０２２９】以上は、３つの主要な機器によりアプリケーション認証システムが構成される場合であったが、図４７に例示されるように、アプリケーション認証システムは、４つの主要な機器により構成されていてもよい。

【０２３０】図４７においては、アプリケーション認証システムは、第１の機器４７０１と、第２の機器４７０２と、第３の機器４７０３と、第４の機器４７０４と、により構成される。第１の機器４７０１は、ＴＲＭ部４７０５と、第１認証処理部４７０６と、を有しており、これらは、図４３に例示されたＴＲＭ部４３０４と、第１認証処理部４３０５と、に対応する。第２の機器４７０２は、第２認証処理部４７０７を有している。これは、図４３に例示された第２認証処理部４３０６に対応する。

【０２３１】第３の機器は、第３認証処理部４７０８を有している。第３認証処理部４７０８は、第２認証処理部４７０７に自身が認証されることを条件として第４の機器４７０４を認証する。第２認証処理部４７０７により第３の機器４７０３が認証されれば、第３の機器４７０３は、第１の機器４７０１にとって信頼できる機器となるので、第１の機器４７０１は、第３の機器４７０３が、ＴＲＭ部４７０５が耐タンパ領域に保持する情報にアクセスすることを許可することができる。そこで、第３認証処理部４７０８は、ＴＲＭ部４７０５が耐タンパ領域に保持する情報を取得し、第４の機器４７０４を認証するようにしてもよい。また、他の機器に保持されている情報を取得し、認証するようにしてもよい。

【０２３２】なお、第３認証処理部４７０８が、ＴＲＭ部４７０５が耐タンパ領域に保持する情報を取得する場合には、第３の機器４７０３と第１の機器４７０１とが直接通信を行なえるようにするために、第３の機器４７０３と第１の機器４７０１とに通信部が備えられていてもよい。あるいは、第２認証処理部４７０７が第１の機器４７０１へアクセスするためのデバイスドライバの機能を備えている場合には、次のようにしてもよい。すなわち、第３認証処理部４７０８は、第２認証処理部４７０７の備えるデバイスドライバの機能を用いて、第２の

機器４７０２を介しながら、ＴＲＭ部４７０５が耐タンパ領域に保持する情報を取得する。したがって、第３認証処理部４７０８は、第２認証処理部４７０７へアクセスするためのデバイスドライバの機能を備えていてもよい。

【０２３３】第４の機器４７０４は、アプリケーション格納部４７０９と、第４認証処理部４７１０と、を有する。アプリケーション格納部４７０９は、図４３のアプリケーション格納部４３０７に対応する。第４認証処理部４７１０は、第３認証処理部４７０８に自身が認証されることを条件として、アプリケーションを認証する。ここで、「自身」とは、第４の機器を意味している。したがって、第３認証処理部４７０８により第４の機器が認証されていれば、第１認証処理部４７０６により認証されたとみなされるので、第４認証処理部は、ＴＲＭ部４７０５が耐タンパ領域に保持する情報を用いて、アプリケーション格納部４７０９に格納されているアプリケーションの認証をすることができる。また、第４認証処理部４７１０は、第３認証処理部４７０８により認証されたことを示す情報を、他の機器に提示して、アプリケーションの認証のための情報を取得して、アプリケーションの認証を行なうようにしてもよい。

【０２３４】このように、４つの主要な機器によりアプリケーション認証システムが構成される場合の動作は次のようになる。第１の機器４７０１の動作は、図４４に例示されたものと同じである。同様に第２の機器４７０２の動作は、図４５に例示されている。第３の機器４７０３の動作は、図４８に例示されているものとなる。すなわち、第３の機器４７０３が第２認証処理部４７０７により認証されたかどうかを、ステップＳ４８０１において、判断する。もし、認証されたのであれば、ステップＳ４８０２において、第４の機器４７０４の認証の処理を行なう。ステップＳ４８０３において、認証ができたかどうかを判断し、もし、認証できたのであれば、ステップＳ４８０４において、第４の機器４７０４へ認証されたことを伝達する。

【０２３５】第４の機器の動作は、図４９に例示されている。第３認証処理部４７０８により認証されたかどうかを、ステップＳ４９０１において、判断し、もし、認証されたのであれば、ステップＳ４９０２において、アプリケーションの認証の処理を行なう。このアプリケーションの認証の処理の結果を、例えば、第１の機器４７０１へ伝達してもよい。また、第２の機器４７０２へも伝達してもよい。また、もし、アプリケーションが他の機器へアクセスする場合には、第３認証処理部４７０８により認証されたことを示す情報を提示するようにしてもよい。あるいは、アプリケーションに第３認証処理部４７０８により認証されたことを示す情報を付加してもよい。

【０２３６】更に、主要な機器の数は４に限定されることなく、図５０に例示されるように、第１の機器５００１と、第２の機器５００２と、第３の機器５００３と、第４の機器５００４と、第５の機器５００５と、の５つの機器によりアプリケーション認証システムが構成されていてもよい。

【０２３７】図５１は、主要な数を一般化した場合のアプリケーション認証システムの機能ブロック図を例示する。図５１において、アプリケーション認証システムは、第１の機器５１０１から第（Ｎ＋１）の機器５１０５までを直列に接続してできる（Ｎ＋１）個の機器により構成される。「接続」と書いたが、これは、電気的に直接接続されていること、あるいは、物理的に接触していることだけを意味しているのではない。例えば、インターネットに代表されるようなネットワークによって接続されていてもよい。特に、光ケーブルを用いたネットワークによって接続されていてもよい。また、無線によって接続されていたりしてもよい。また、それぞれの機器が相互に接続されていてもよい。

【０２３８】第１の機器５１０１は、ＴＲＭ部５１０１と第１認証処理部５１０２と、を有している。ＴＲＭ部５１０１は、第２の機器５１０２を認証するための情報である認証情報を耐タンパ領域に保持する。第１認証処理部５１０２は、認証情報に基づいて第２の機器５１０２を認証する。

【０２３９】以下では、第２の機器５１０２から第Ｎの機器までのいずれか一の機器を第ｉの機器と表記することにする。第ｉの機器は、第ｉ認証処理部を有する。第ｉ認証処理部は、第（ｉ－１）認証処理部に自身が認証されることを条件として第（ｉ＋１）の機器を認証する。ここに「自身」とは、第ｉの機器を意味する。したがって、第ｉ認証処理部は、第ｉの機器が第（ｉ－１）認証処理部に認証されているならば、第（ｉ＋１）の機器を認証する。第ｉの機器が第（ｉ－１）認証処理部に認証されているならば、第１の機器５１０１にとって、第ｉの機器は信頼できるとみなすことができるので、第１の機器５１０１は、第ｉの機器が、ＴＲＭ部５１０１により耐タンパ領域に保持されている情報にアクセスを許すことができる。そこで、第ｉの機器は、耐タンパ領域に保持された情報を用いて、第（ｉ＋１）の機器を認証するようにしてもよい。

【０２４０】例えば、第ｉ認証処理部が、ＴＲＭ部５１０７により耐タンパ領域に保持されている情報にアクセスする場合には、第ｉの機器と第１の機器とが直接通信を行なうようにしてもよい。

【０２４１】また、第ｉ認証処理部は、第（ｉ－１）認証処理部へアクセスするためのデバイスドライバなどの機能を備えていてもよい。この備えられた機能により、情報の要求が第ｉ認証処理部から第１認証処理部５１０７へ順に出力され、要求された情報が第１認証処理部５１０７から第ｉ認証処理部へ順に返信されるようにな

る。

【０２４２】第（Ｎ＋１）の機器５１０５は、アプリケーション格納部５１１１と、第（Ｎ＋１）認証処理部５１１２と、を有している。アプリケーション格納部５１１１は、アプリケーションを格納する。アプリケーションを格納している時間は特に問わず、例えば、第（Ｎ＋１）の機器５１０５にてアプリケーションを実行するためにアプリケーションが格納されるようになっていてもよいし、アプリケーションの伝達を中継するためだけに一時的に格納されるようになっていてもよい。また、格納の目的も特に問わず、第（Ｎ＋１）の機器５１０５にてアプリケーションを実行する場合のみならず、他の機器でのアプリケーションの実行のためのダウンロードの目的に格納してもよい。また、第（Ｎ＋１）の機器５１０５でアプリケーションをダウンロードして実行する目的で格納してもよい。なお、アプリケーションという名称を用いたが、プログラムである必要はなく、データであってもよい。

【０２４３】第（Ｎ＋１）認証処理部５１１２は、第Ｎ認証処理部に自身が認証されることを条件として、アプリケーションを認証する。「自身」とは、第（Ｎ＋１）の機器５１０５を意味し、「アプリケーション」とは、アプリケーション格納部５１１１に格納されたアプリケーションを意味する。

【０２４４】第１の機器５１０１の動作を説明するフローチャートは、図４４に例示されている。

【０２４５】図５２は、第２の機器から第Ｎの機器までのいずれか一の機器の動作を説明するフローチャートである。ステップＳ５２０１において、第（ｉ－１）認証処理部により認証されたかどうかを判断し、もし、認証されれば、第（ｉ＋１）の機器の認証の処理をステップＳ５２０２において行なう。第（ｉ＋１）の機器が認証されたかどうかを、ステップＳ５２０３において、判断し、もし、認証されたのであれば、第（ｉ＋１）の機器へ認証されたことを伝達する。これにより、第２の機器から順に認証が第Ｎの機器までが認証されることになる。

【０２４６】図５３は、第（Ｎ＋１）の機器５１０５の動作のフローチャートを例示している。第Ｎ認証処理部５１０５により認証されたかどうかをステップＳ５３０１において判断し、もし認証されたと判断されれば、ステップＳ５３０２において、アプリケーションの認証の処理を行なう。アプリケーションの認証ができれば、その結果を第１の機器５１０１などへ伝達し、アプリケーションによる第１の機器５１０１へのアクセスすることを許可するようにする。あるいは、認証がされたということを示す情報をアプリケーションに付加するようにしてもよい。

【０２４７】図４３、図４７、図５０、図５１においては、機器が直列に接続されていたが、入れ子構造を用いて機器が接続されていてもよい。図５４は、入れ子構造を用いて機器が接続されていることを模式的に例示している。セキュアデバイス５４０１が第１の機器に相当し、ＴＲＭ部と第１認証処理部とを有する。セキュアデバイス５４０２は、第２の機器に相当するアダプタ５４０２の一部として組み込まれるように接続される。アダプタ５４０２は、第３の機器に相当する通信モジュール５４０３の一部として組み込まれるように接続されている。さらに通信モジュール５４０３は、第４の機器に相当するＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｃｅ）５４０４の一部として組み込まれるように接続される。ＰＤＡ５４０４は、サーバ５４０５と通信回線などを通じて第５の機器に相当するサーバに接続される。このように接続が行なわれることにより、例えば、サーバ５４０５に格納されたアプリケーションを、セキュアデバイス５４０１の耐タンパ領域に保持された情報を用いて認証することができる。

【０２４８】なお、第（Ｎ＋１）の機器５１０５は、例えば、家庭用電化製品であってもよい。また、いわゆる、情報家電やネット家電と呼ばれるものであってもよい。そのような家庭電化製品を例示列挙すれば、エアコンディショナ、加湿器、除湿器、空気清浄機、電子レンジ、オーブン、冷蔵庫、食器洗い機、湯沸し器、アイロン、ズボンプレッサー、電気掃除機、洗濯機、乾燥機、電気毛布、電気敷布、照明機器、テレビ受像機、ラジオ受信機、テープレコーダなどのオーディオ機器、カメラ、ＩＣレコーダ、電話機、ファクシミリ送受信機、コピー機、プリンター、スキャナー、パーソナルコンピュータ、などを挙げることができる。

【０２４９】（実施の形態２１）実施の形態２０においては、第２の機器から第Ｎの機器までのいずれか一を第ｉの機器と表記するとき、第ｉの機器は、第（ｉ＋１）の機器の認証を行なうために必要な情報を保持するようになっていてもよい。例えば、第ｉの機器が耐タンパ領域を有し、そこに認証を行なうのに必要な情報を保持していてもよい。

【０２５０】このように第ｉの機器が認証を行なうために必要な情報である認証情報を保持している場合があり得るとき、第ｉの機器が第ｉ認証情報取得部を有していてもよい。ここに、第ｉ認証情報取得部とは、第ｉの機器が認証情報を格納している領域である認証情報格納領域を有している場合には、その認証情報格納領域から認証情報を取得する部である。また、第ｉ認証情報取得部は、第１の機器のＴＲＭ部に認証情報が格納されている場合には、第２の機器から第（ｉ－１）の機器までの機器を介して、ＴＲＭ部から認証情報を取得する。「第２の機器から第（ｉ－１）の機器までの機器を介して」とは、次を意味する。すなわち、第ｉ認証情報取得部が、第（ｉ－１）認証情報取得部へ認証情報の要求を出力し、最後には、第２認証情報取得部が第１の機器へ認証

情報の要求を出力する。第２認証情報取得部が第１の機器から認証情報を取得すると、第３認証情報取得部へ認証情報を出力し、最後には、第（ｉ－１）認証情報取得部が第ｉ認証情報取得部へ認証情報を出力する。

【０２５１】図５５は、本実施の形態における第ｉの機器の動作を説明するフローチャートを例示する。ステップＳ５５０１において、第（ｉ－１）認証処理部により認証されたかどうかを判断する。認証されたと判断されれば、ステップＳ５５０２へ処理が移され、認証情報格納領域に、第（ｉ＋１）の機器の認証情報が格納されているかどうかを判断する。例えば、認証情報格納領域に格納されている情報を読み出し、認証情報が得られるかどうかを判断する。もし、格納されていなければ、ステップＳ５５０３へ処理が移され、第２の機器から第（ｉ－１）の機器までを介してＴＲＭ部より認証情報を取得する。ステップＳ５５０４において、第（ｉ＋１）の機器の認証の処理を行ない、認証できたかどうかをステップＳ５５０５において判断する。もし、認証できたのであれば、ステップＳ５５０６において、第（ｉ＋１）の機器へ認証されたことを伝達する。

【０２５２】このような処理を行なうことにより、アプリケーション認証システムを構成する機器の数が増えても、機器が認証情報を持っていれば、その認証情報を使用して認証がされるので、例えば、全ての機器の認証の時間を短時間に終わらせることが可能となる。

【０２５３】

【発明の効果】以上のように本発明によれば、認証モジュールと端末とを組み合わせ、端末内で動作するアプリケーションを認証モジュールの持つ情報で認証することにより、好ましくないアプリケーションが端末内で実行されてしまうことを防止することができる。

【０２５４】また、端末内のＴＲＭアクセスライブラリが認証モジュールによって認証されることにより、ＴＲＭアクセスライブラリがアプリケーションの認証のための処理を行なうことが可能となる。この結果、高いセキュリティを伴うアプリケーションの実行が可能となり、端末を用いた商取引の操作が可能となる。また、耐タンパ領域は認証モジュールにあればよく、端末に耐タンパ領域を実装する必要がなくなるので、端末の製造コストを下げることができる。

【０２５５】また、端末内で動作するアプリケーションが認証されることにより、アプリケーションの出所が保証され、端末や認証モジュールのローカルリソースのアクセスをアプリケーションに許可することができる。

【０２５６】また、サーバが認証モジュールのＴＲＭ部を認証することにより、端末を認証すること、および、端末内で動作するアプリケーションの認証を行なうことができるので、機密性の高い情報を端末内で動作するアプリケーションと交換することができ、複雑な商取引の操作をサーバ、端末、認証モジュール間で実現することができる。

【０２５７】また、オプショナル領域にアプリケーション本体の署名を格納することにより、アプリケーションのダウンロードと同時にアプリケーション本体の署名をダウンロードすることが可能となり、別にアプリケーション本体の署名をダウンロードする手間を省くことができる。

【０２５８】また、３つ以上の機器が直列に接続された状態で、一方の端の機器から順次認証を行ない、他の端の機器に格納されたアプリケーションの認証が可能となる。

【図面の簡単な説明】

【図１】実施の形態１におけるアプリケーション認証システムの機能ブロック図

【図２】実施の形態１におけるアプリケーション認証システムの実施例を示す図

【図３】実施の形態１におけるアプリケーション認証システムの実施例を示す図

【図４】実施の形態２におけるアプリケーション認証システムの機能ブロック図

【図５】実施の形態２におけるアプリケーション認証システムの機能ブロック図

【図６】アプリケーション本体と署名との関係を説明する図

【図７】実施の形態２における端末の動作を説明するフローチャート

【図８】実施の形態２における認証モジュールの動作を説明するフローチャート

【図９】実施の形態３における認証モジュールの機能ブロック図

【図１０】実施の形態３における認証モジュールの動作を説明するフローチャート

【図１１】実施の形態４におけるアプリケーション認証システムの機能ブロック図

【図１２】実施の形態４における認証モジュールを端末が認証する処理を説明するフローチャート

【図１３】実施の形態５におけるアプリケーション認証システムの機能ブロック図

【図１４】アプリケーション利用リソース情報を模式的に表す図

【図１５】アプリケーション利用リソース情報がアプリケーションと共にダウンロードされる状態を模式的に表す図

【図１６】実施の形態６におけるアプリケーション認証システムの機能ブロック図

【図１７】実施の形態７におけるアプリケーション認証システムの機能ブロック図

【図１８】実施の形態８におけるアプリケーション認証システムの機能ブロック図

【図１９】実施の形態８における端末の動作を説明する

フローチャート

【図２０】実施の形態８における認証モジュールの動作を説明するフローチャート

【図２１】実施の形態９におけるアプリケーション認証システムの機能ブロック図

【図２２】実施の形態９における認証モジュールの動作を説明するフローチャート

【図２３】実施の形態９における認証モジュールの動作を説明するフローチャート

【図２４】実施の形態９におけるアプリケーション認証システムの機能ブロック図

【図２５】実施の形態９をＩＣカードにおいて実現する例を示す図

【図２６】実施の形態９をＩＣカードにおいて実現する例を示す図

【図２７】実施の形態１０におけるアプリケーション認証システムの機能ブロック図

【図２８】実施の形態１１におけるアプリケーション認証システムの機能ブロック図

【図２９】実施の形態１２におけるアプリケーション認証システムの機能ブロック図

【図３０】実施の形態１２におけるアプリケーション認証システムの動作を説明するシーケンス図

【図３１】実施の形態１３におけるアプリケーション認証システムの機能ブロック図

【図３２】実施の形態１３におけるアプリケーション認証システムの動作を説明するシーケンス図

【図３３】実施の形態１４におけるアプリケーション認証システムの機能ブロック図

【図３４】ＪＡＶＡ（登録商標）アプリケーションのアプリケーション本体とアプリケーション定義ファイルを模式的に示す図

【図３５】オプショナル領域に格納された署名を用いてアプリケーションの認証を行なう処理を説明するフローチャート

【図３６】実施の形態２のアプリケーション認証システムのＴＲＭアクセスライブラリ部がアプリケーションマネージャとデバイスドライバとを備えている図

【図３７】実施の形態１６の端末の機能ブロック図

【図３８】実施の形態１７の端末の機能ブロック図

【図３９】実施の形態１７の端末における処理の流れを＊説明するフローチャート

【図４０】実施の形態１８におけるアプリケーション認証システムの機能ブロック図

【図４１】実施の形態１９におけるアプリケーション認証システムの機能ブロック図

【図４２】実施の形態１９におけるアプリケーション認証システムの処理の流れを説明するフローチャート

【図４３】３つの機器より構成されるアプリケーション認証システムの機能ブロック図

【図４４】第１の機器の動作の流れを説明するフローチャート

【図４５】第２の機器の動作の流れを説明するフローチャート

【図４６】アプリケーション認証システムが３つの機器より構成される場合における第３の機器の動作の流れを説明するフローチャート

【図４７】４つの機器より構成されるアプリケーション認証システムの機能ブロック図

【図４８】アプリケーション認証システムが４つの機器より構成される場合における第３の機器の動作の流れを説明するフローチャート

【図４９】アプリケーション認証システムが４つの機器より構成される場合における第４の機器の動作の流れを説明するフローチャート

【図５０】５つの機器より構成されるアプリケーション認証システムの機能ブロック図

【図５１】Ｎ＋１の機器より構成されるアプリケーション認証システムの機能ブロック図

【図５２】第ｉの機器の動作の流れを説明するフローチャート

【図５３】第（Ｎ＋１）の機器の動作の流れを説明するフローチャート

【図５４】入れ子構造を用いて機器が接続されていることを示す模式図

【図５５】実施の形態２１における第ｉの機器の動作の流れを説明するフローチャート

【符号の説明】

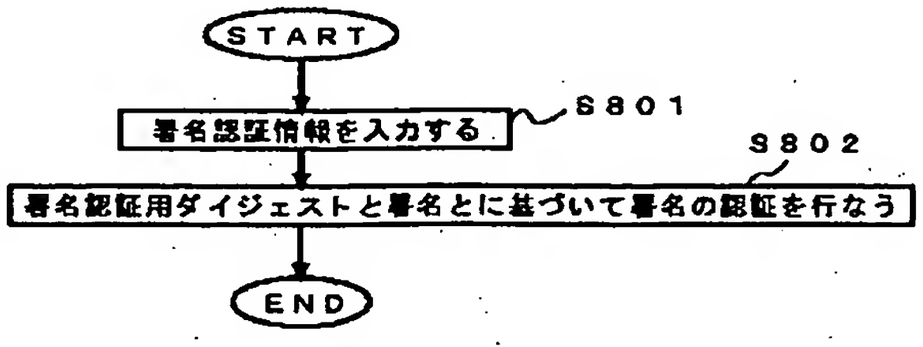
１００　端末

１０１　認証モジュール

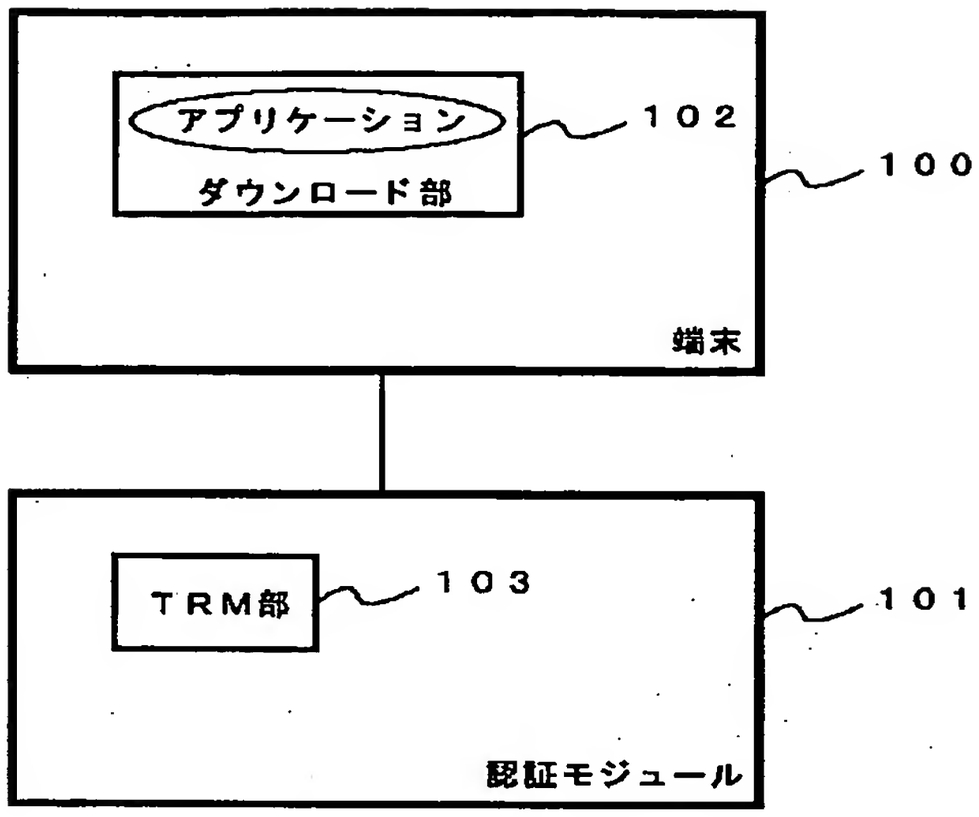
１０２　ダウンロード部

１０３　ＴＲＭアクセス部

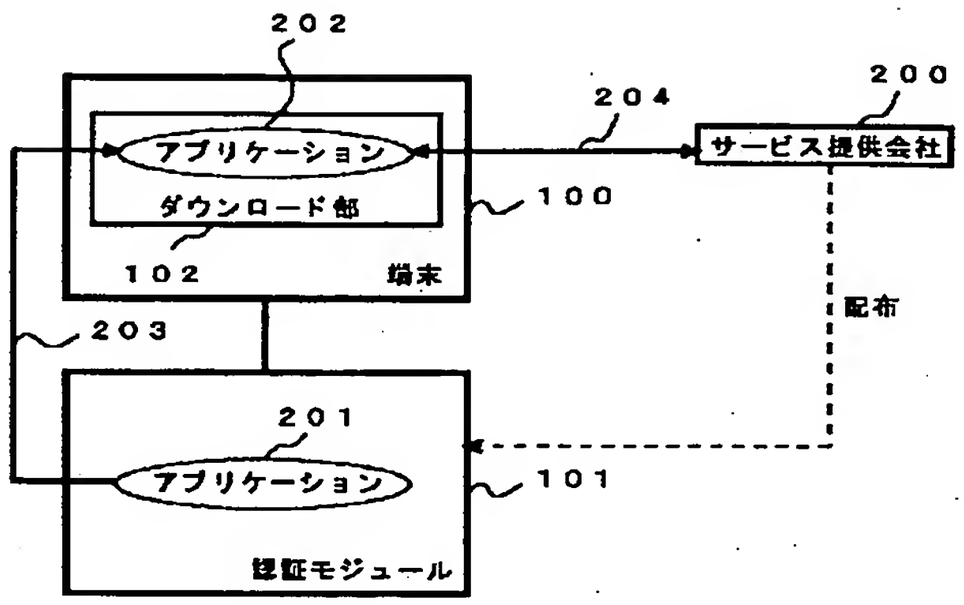
【図８】



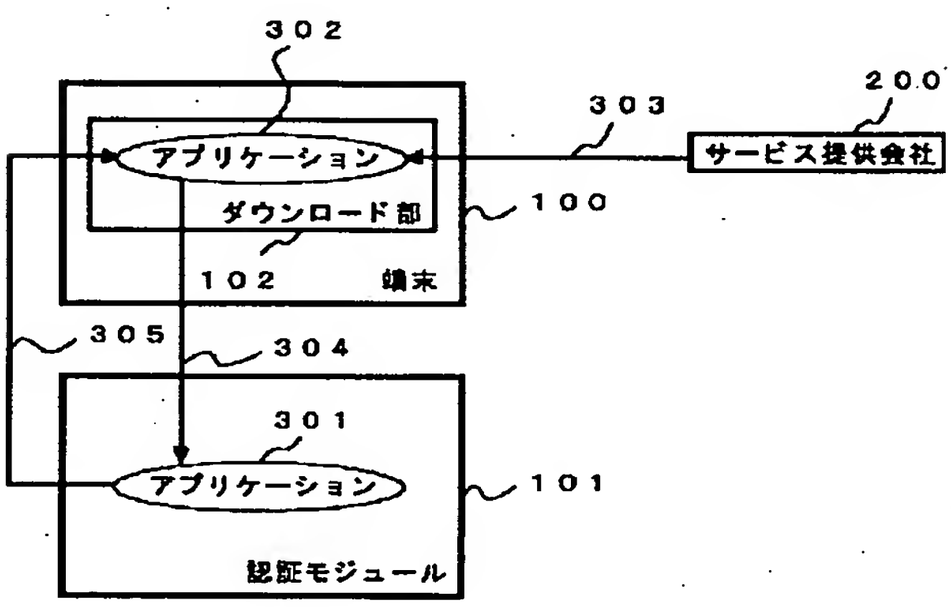
【図１】



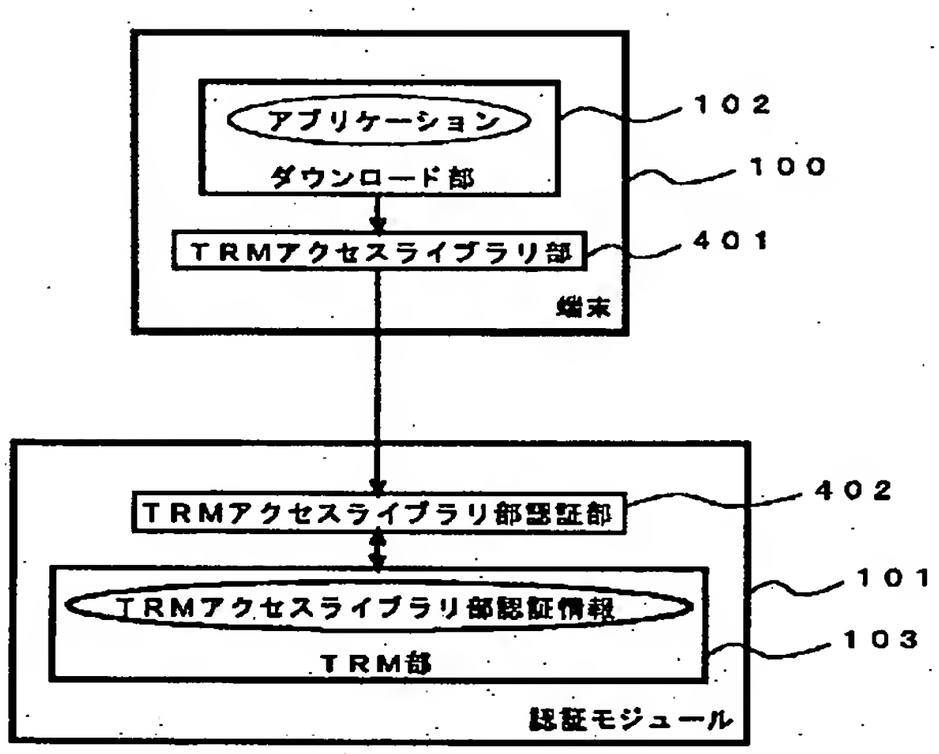
【図２】



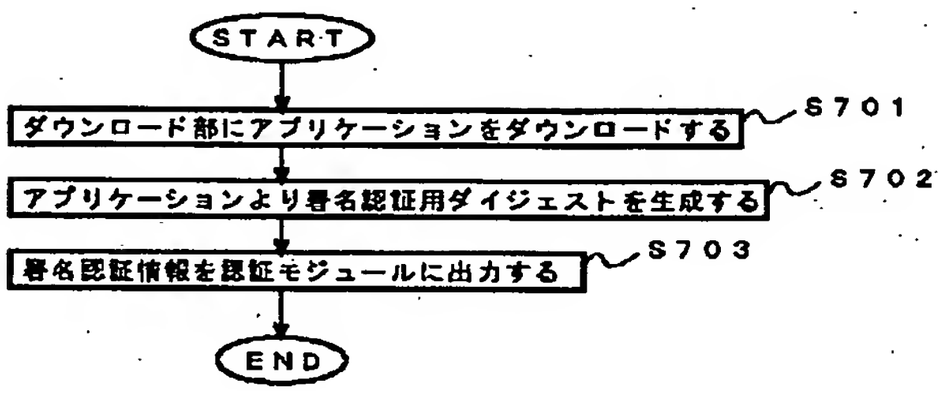
【図３】



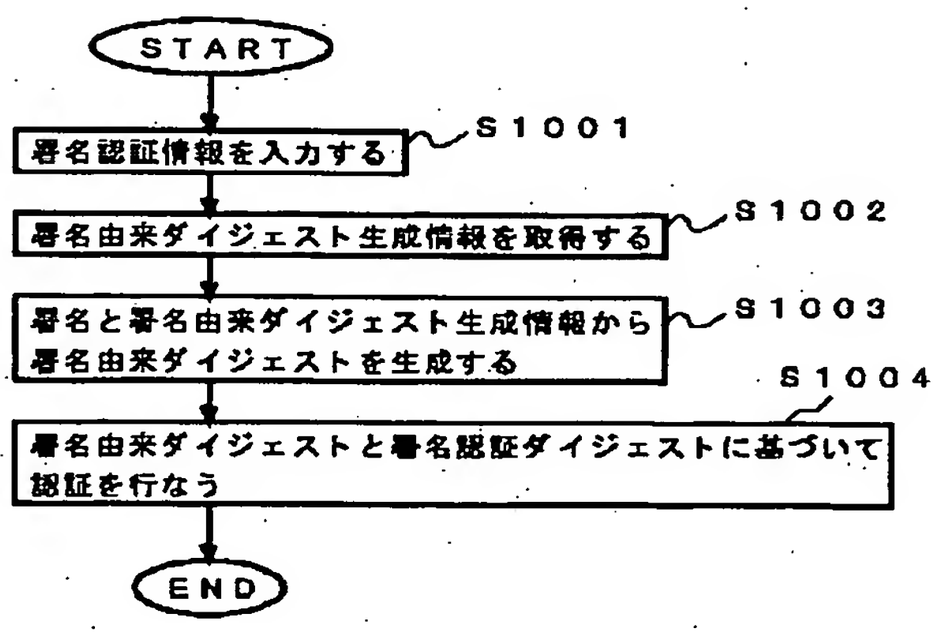
【図４】



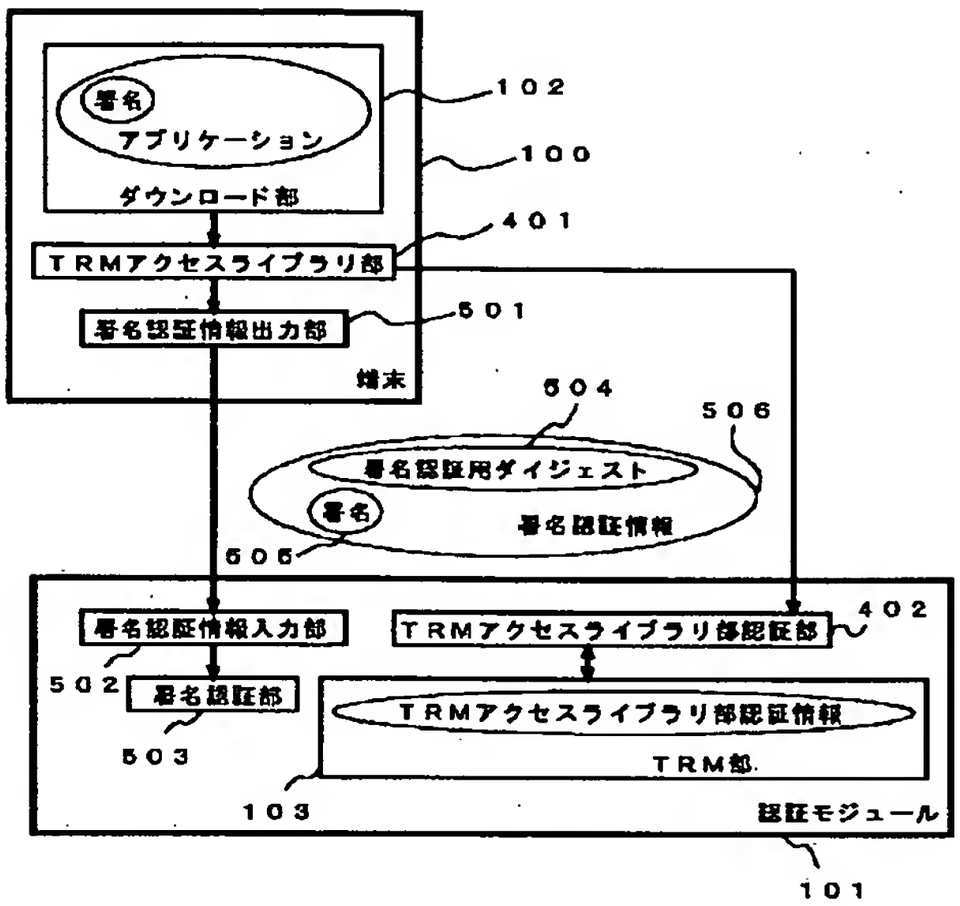
【図７】



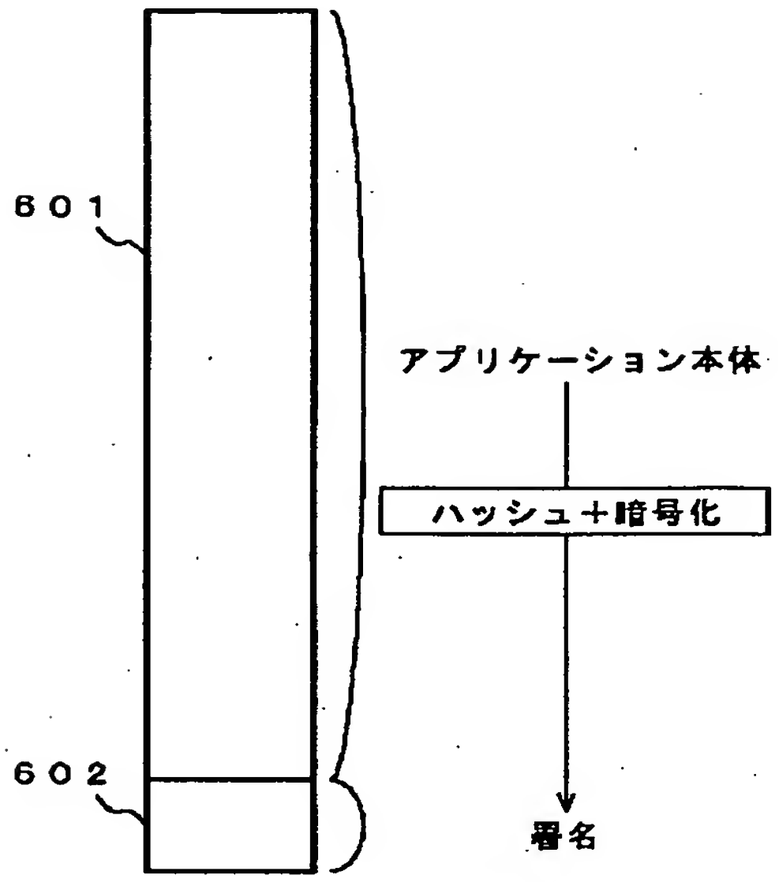
【図１０】



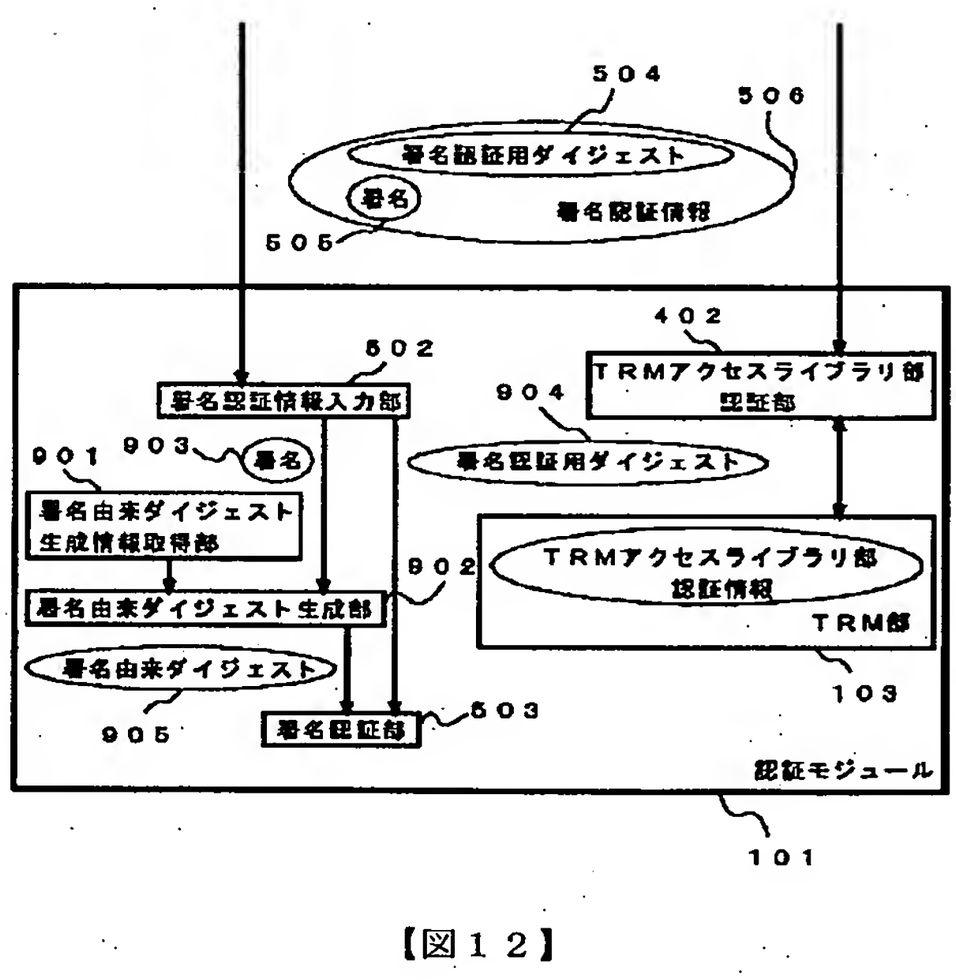
【図５】



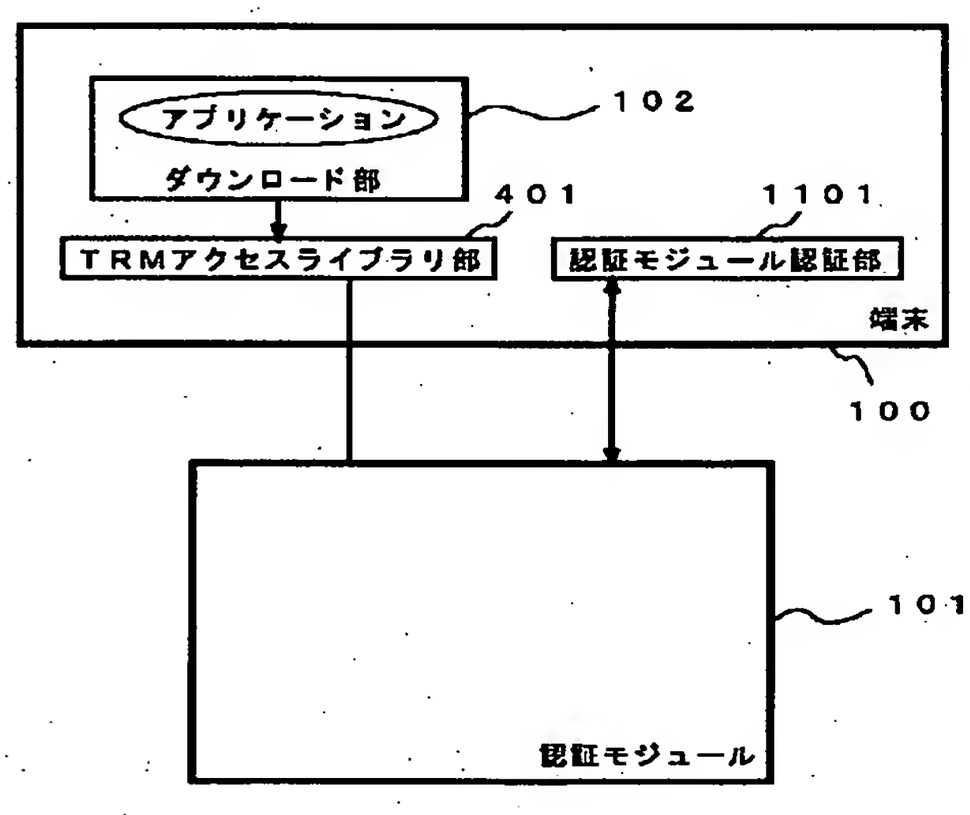
【図６】



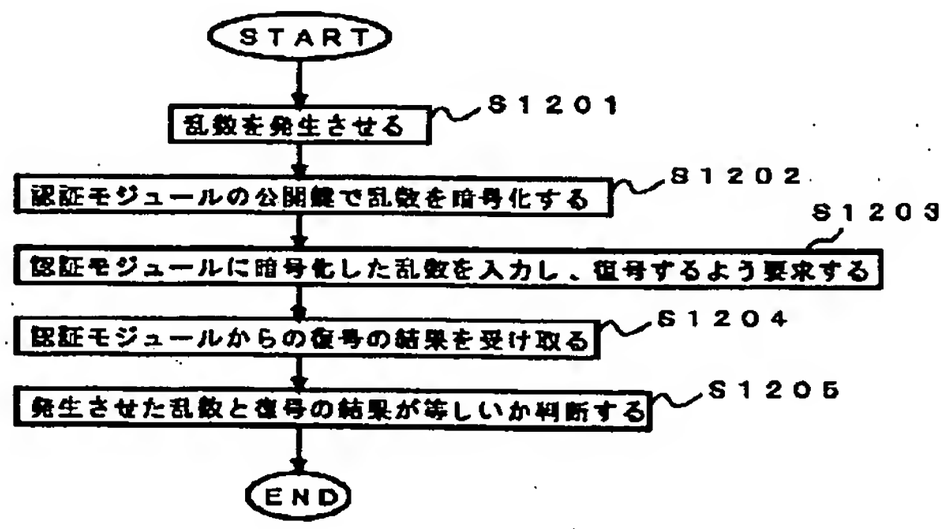
【図９】



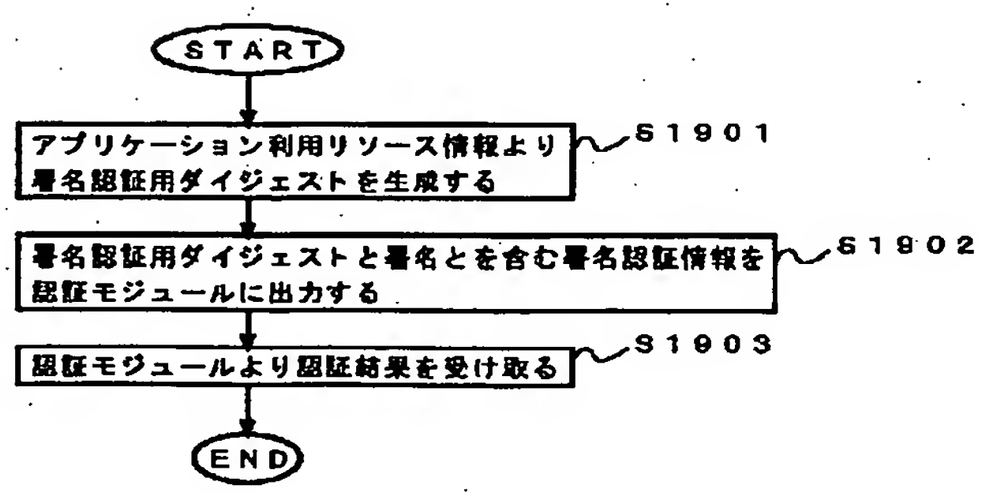
【図１１】



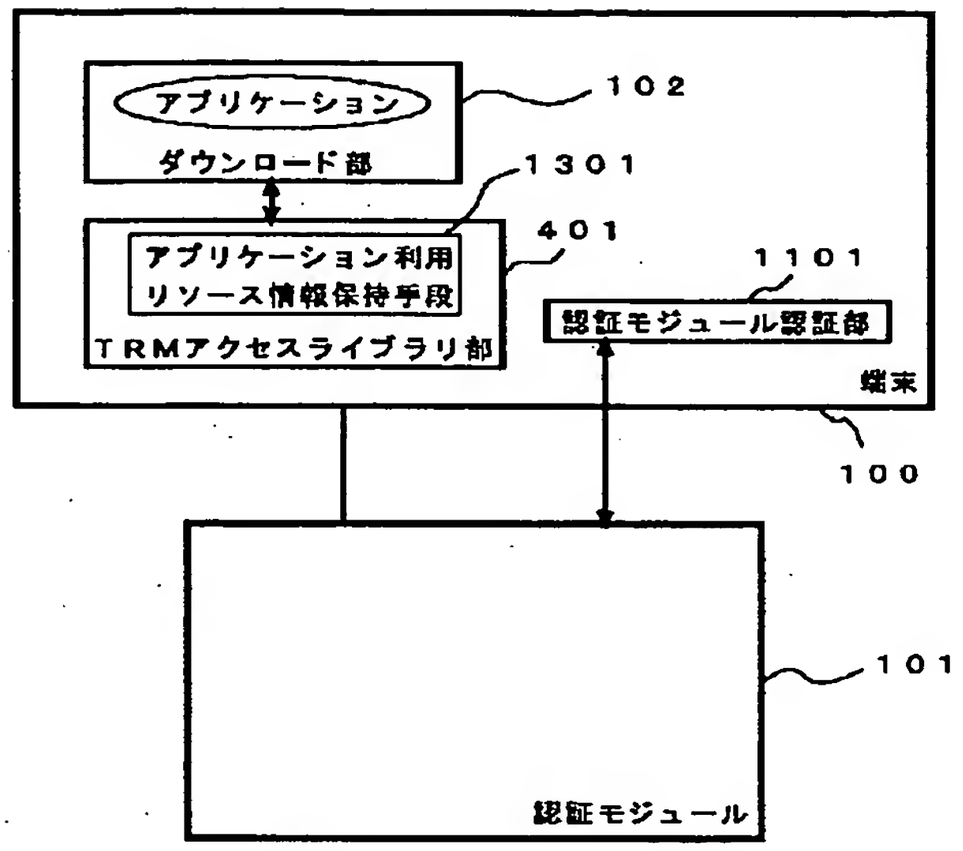
【図１２】



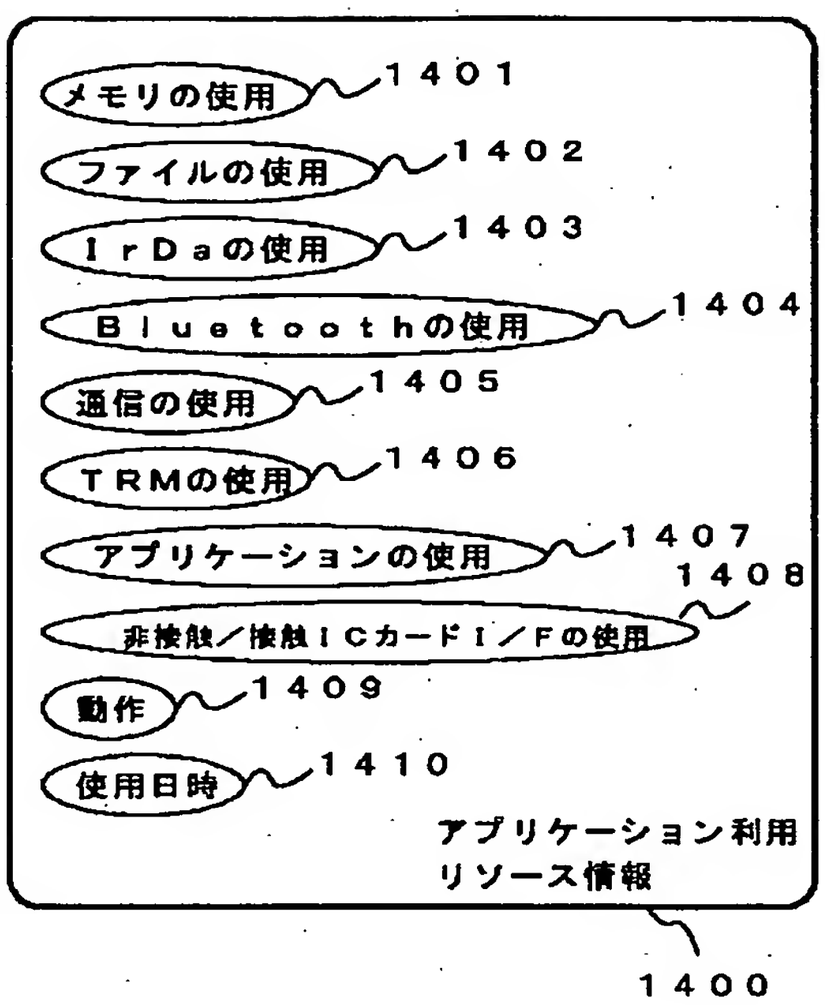
【図１９】



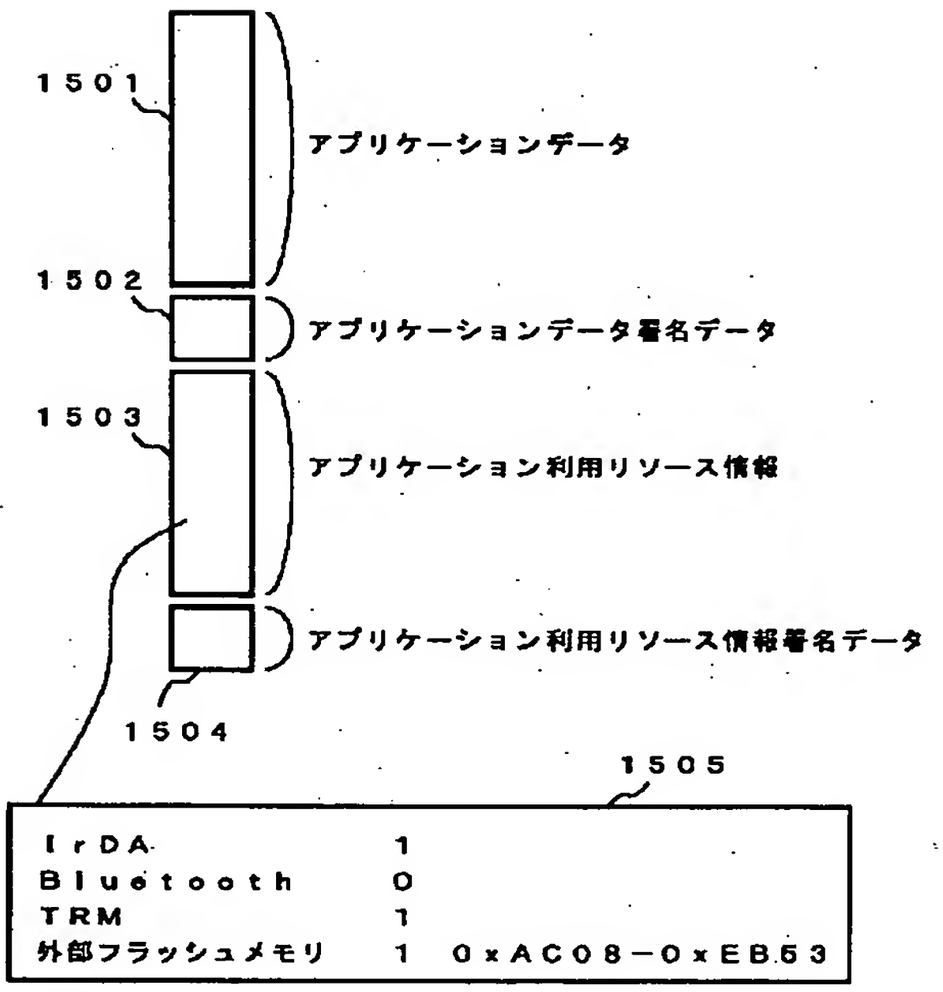
【図１３】



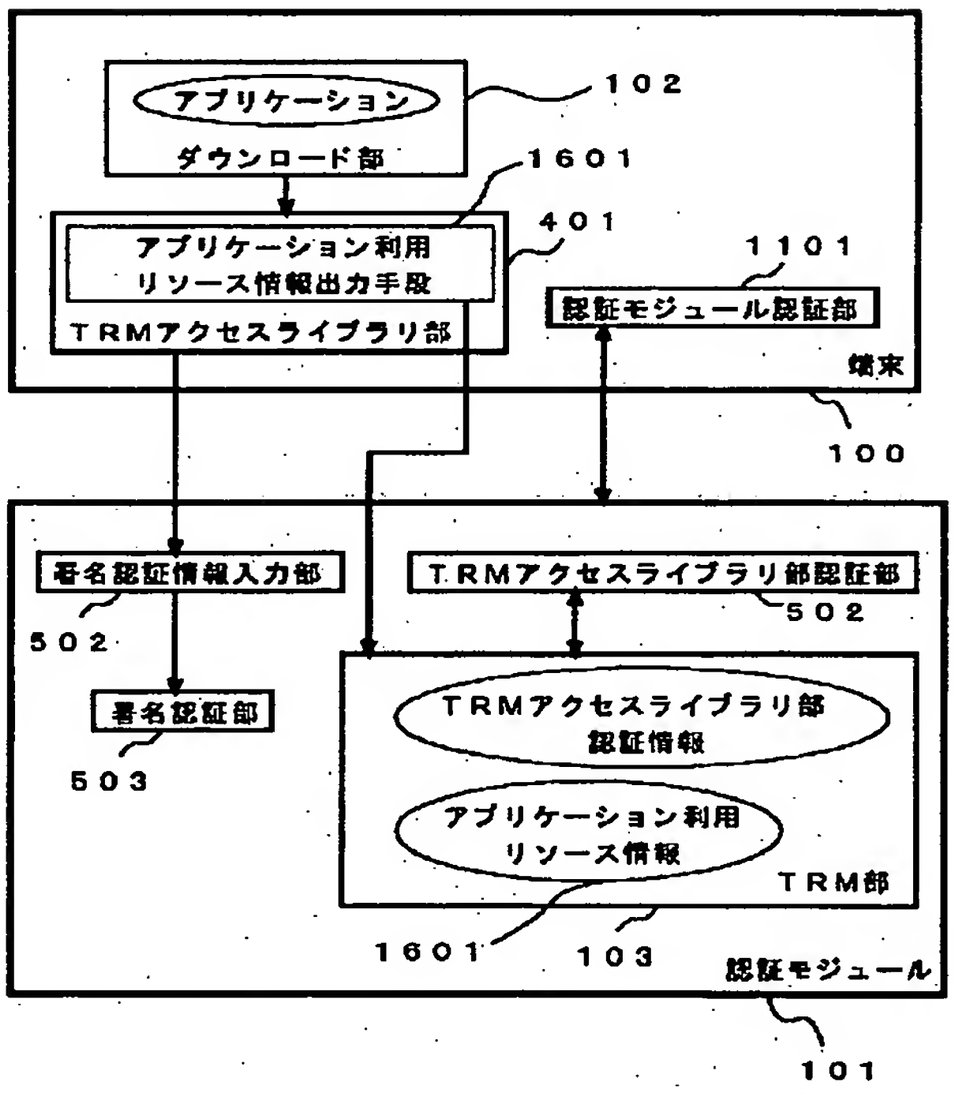
【図１４】



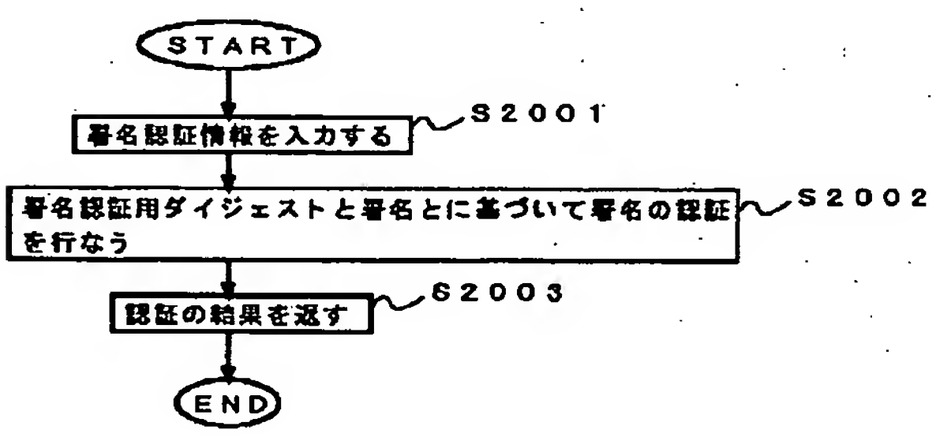
【図１５】



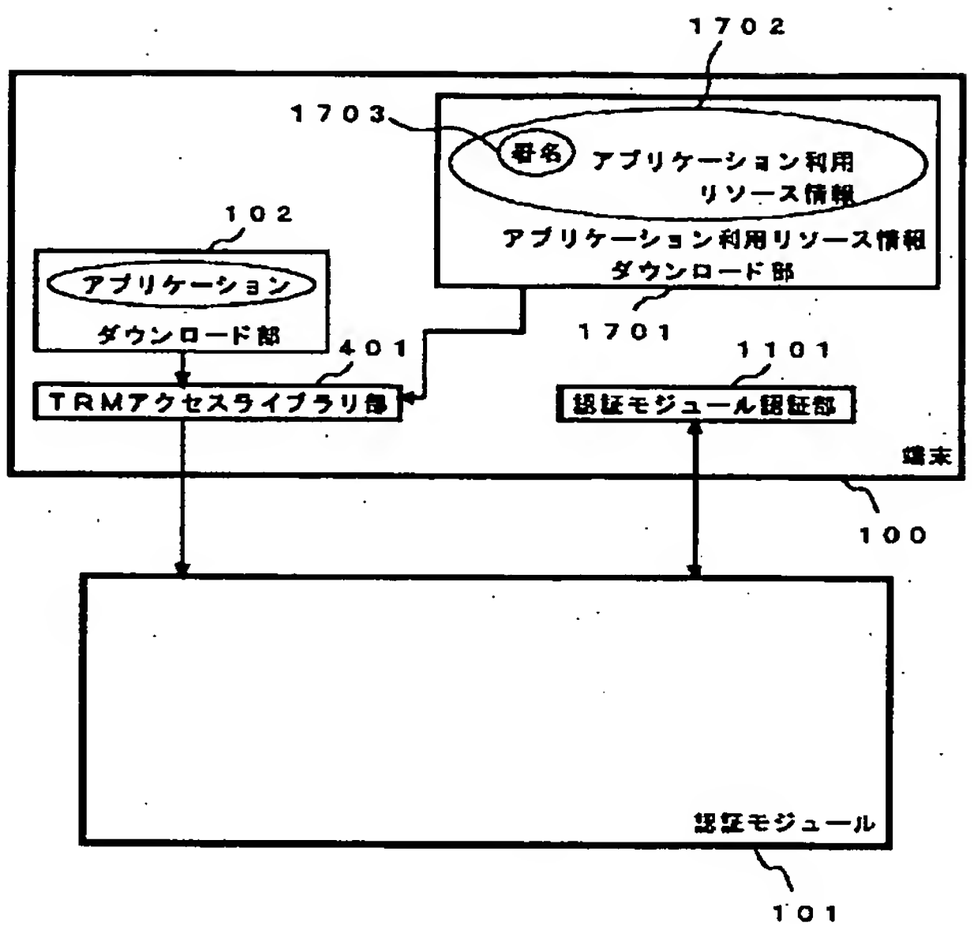
【図１６】



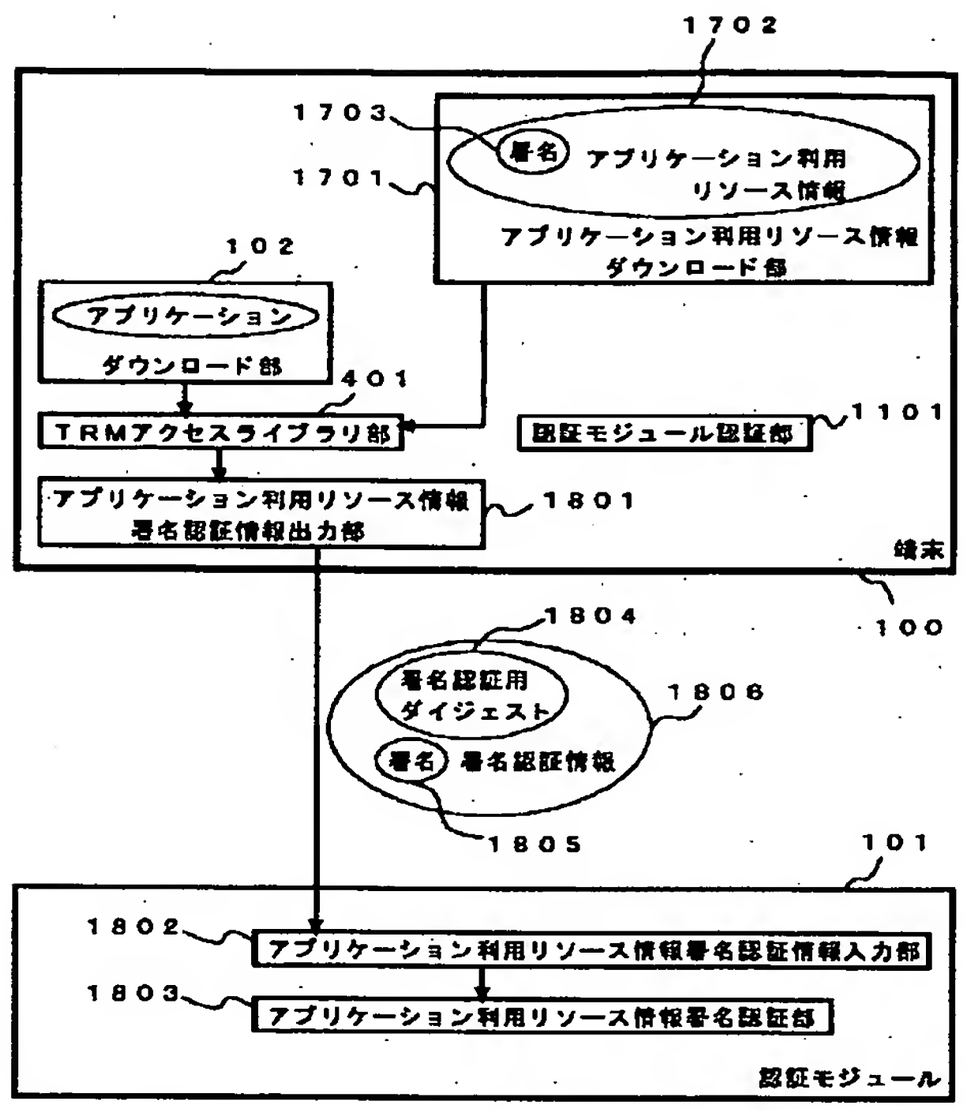
【図２０】



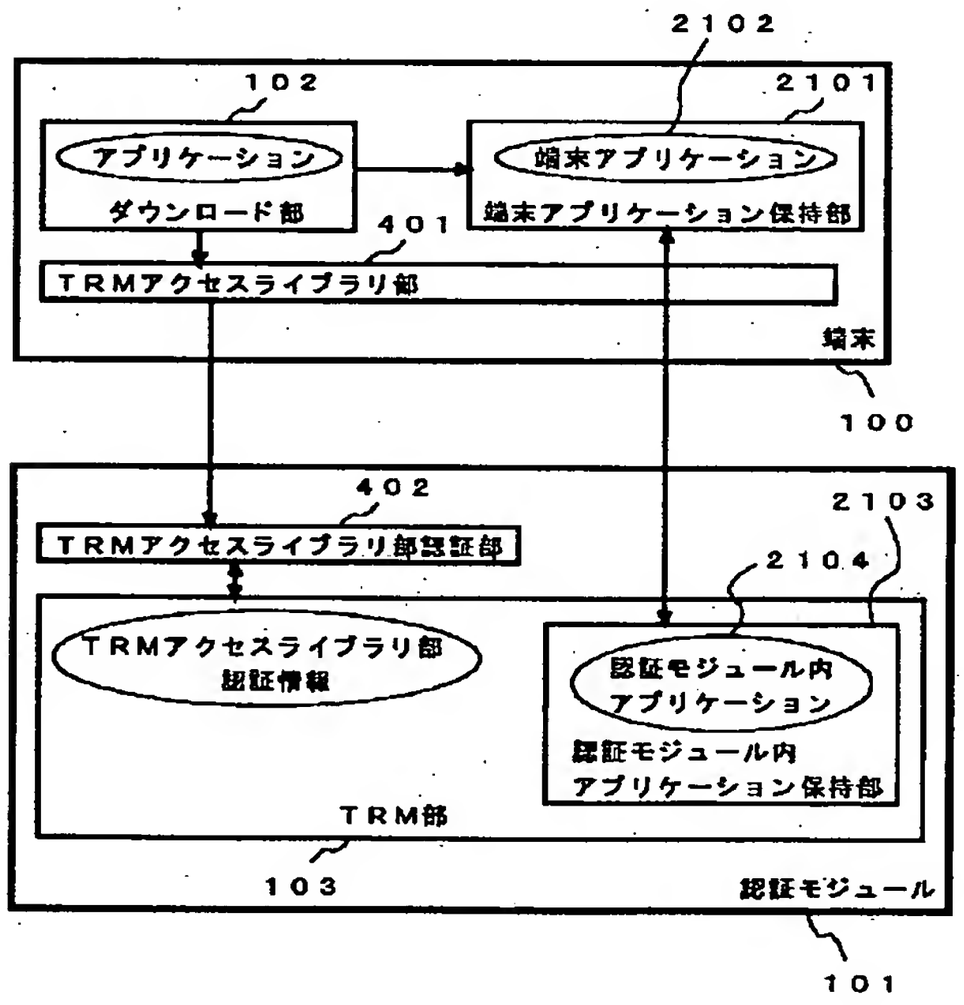
【図１７】



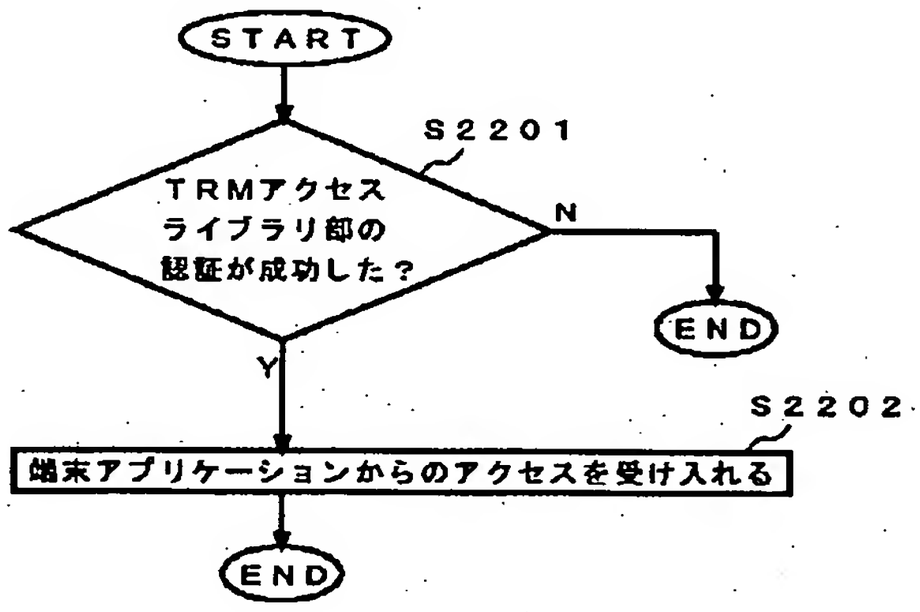
【図１８】



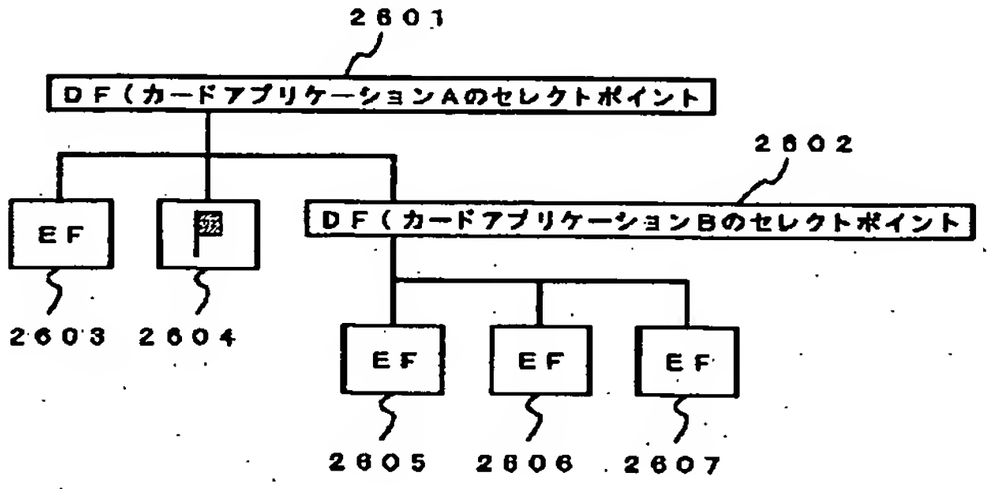
【図２１】



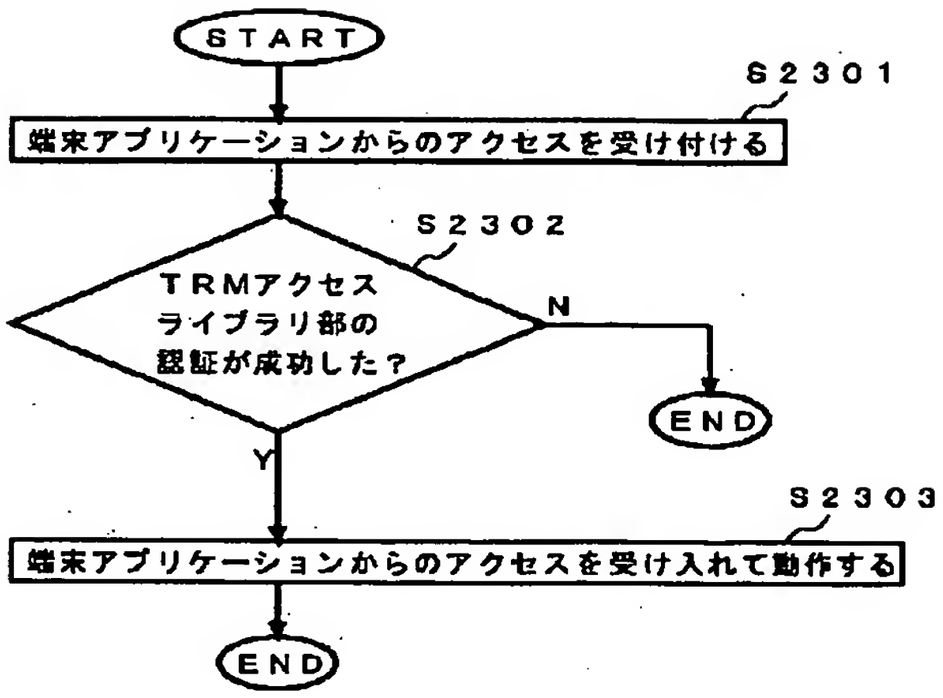
【図２２】



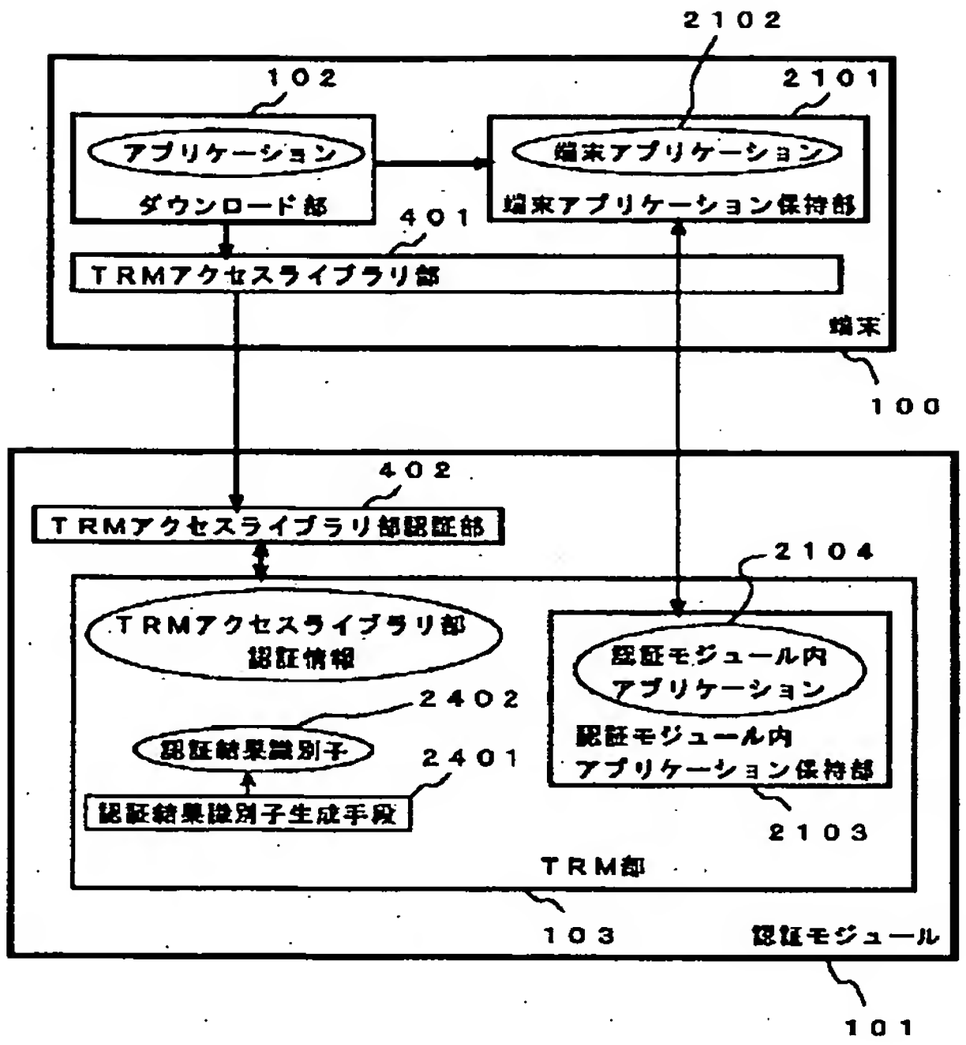
【図２６】



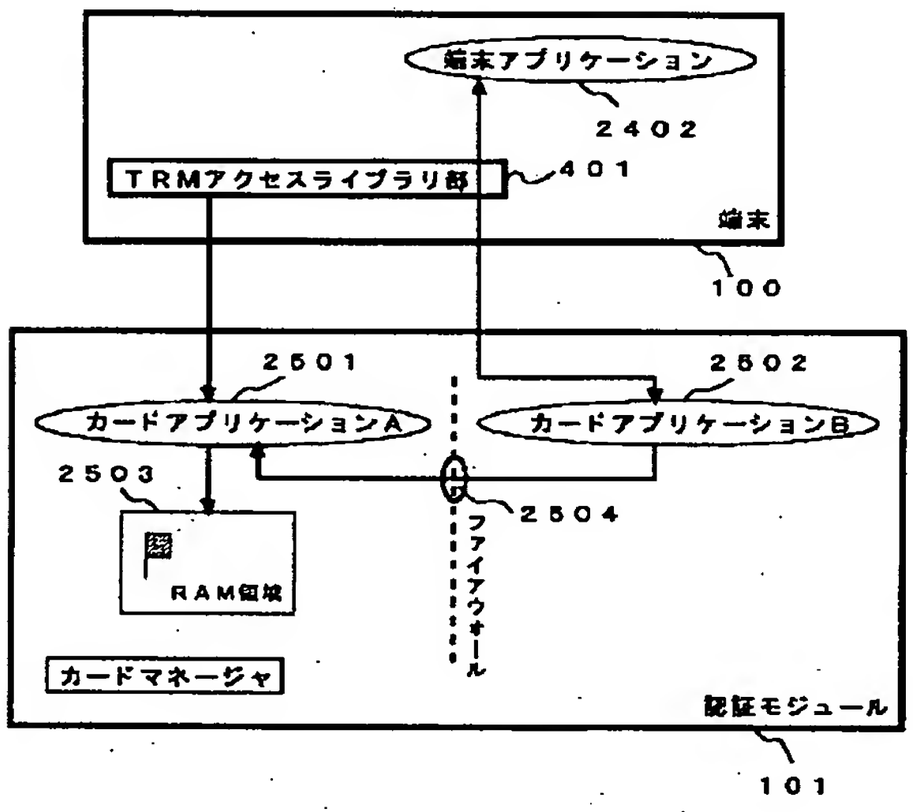
【図２３】



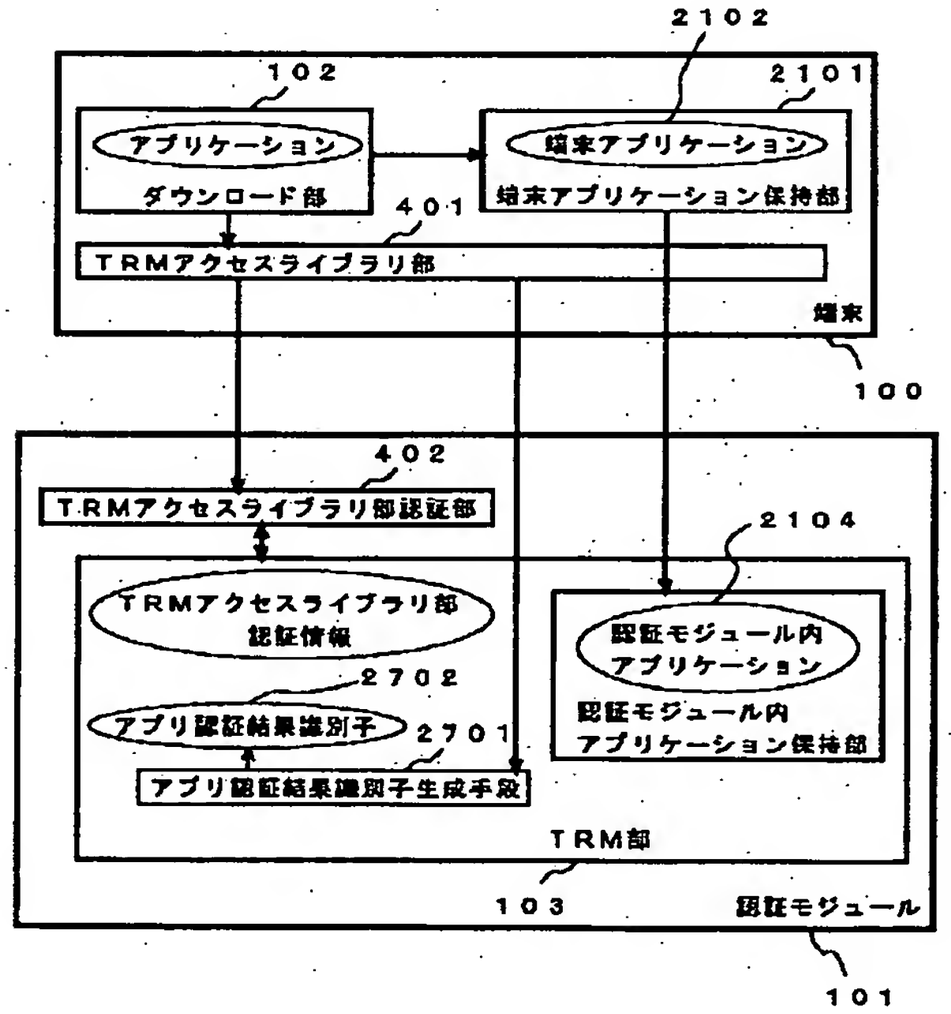
【図２４】



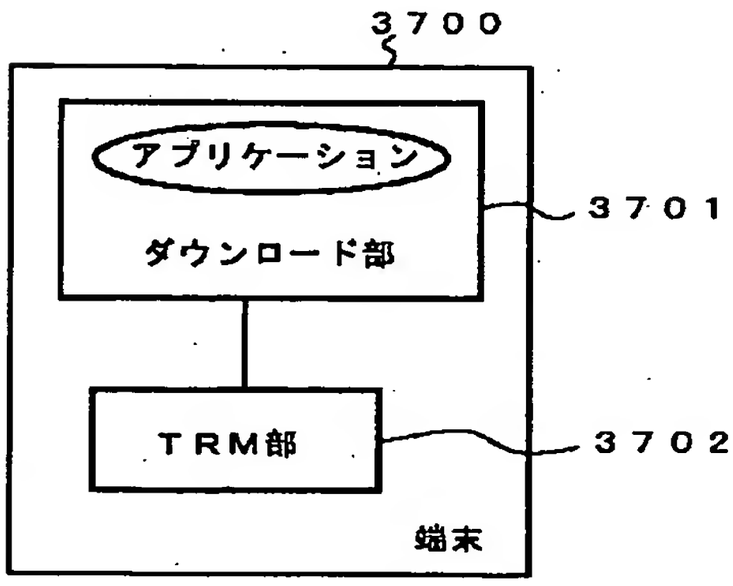
【図２５】



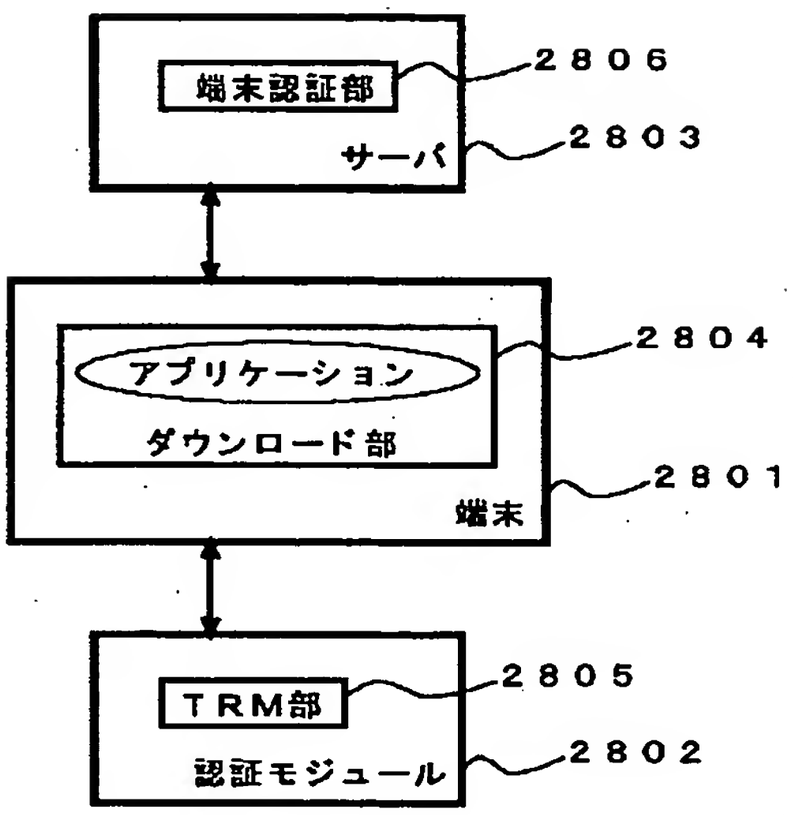
【図２７】



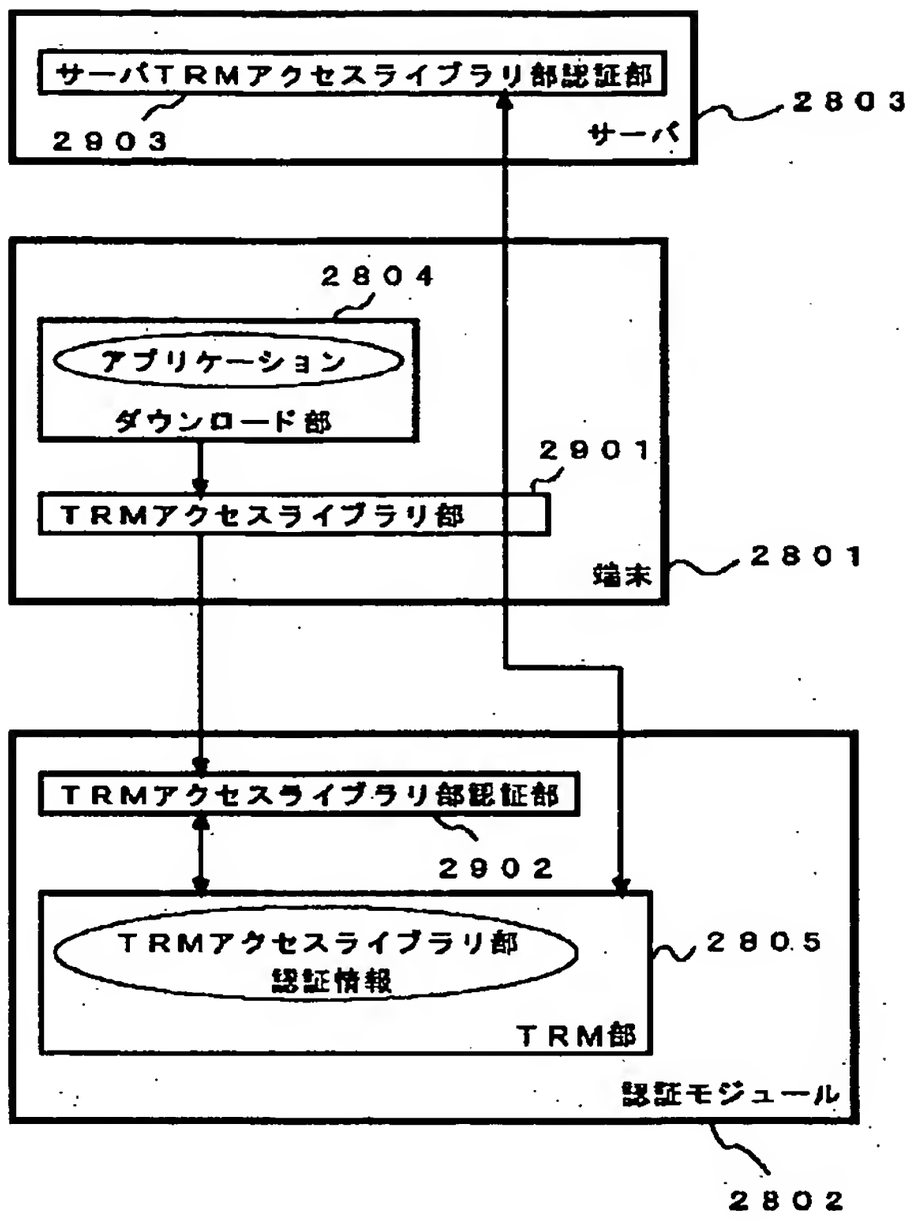
【図３７】



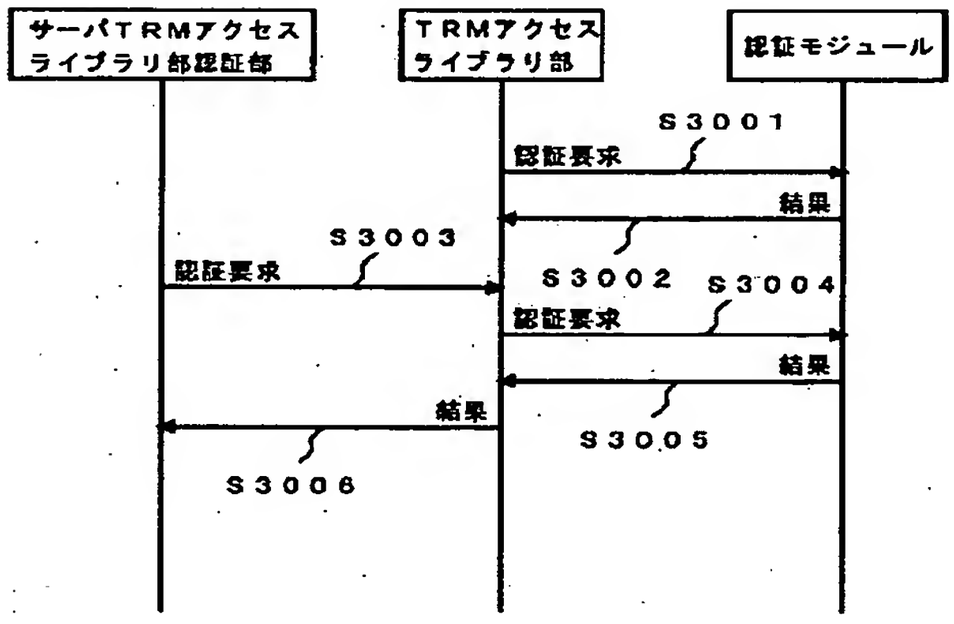
【図２８】



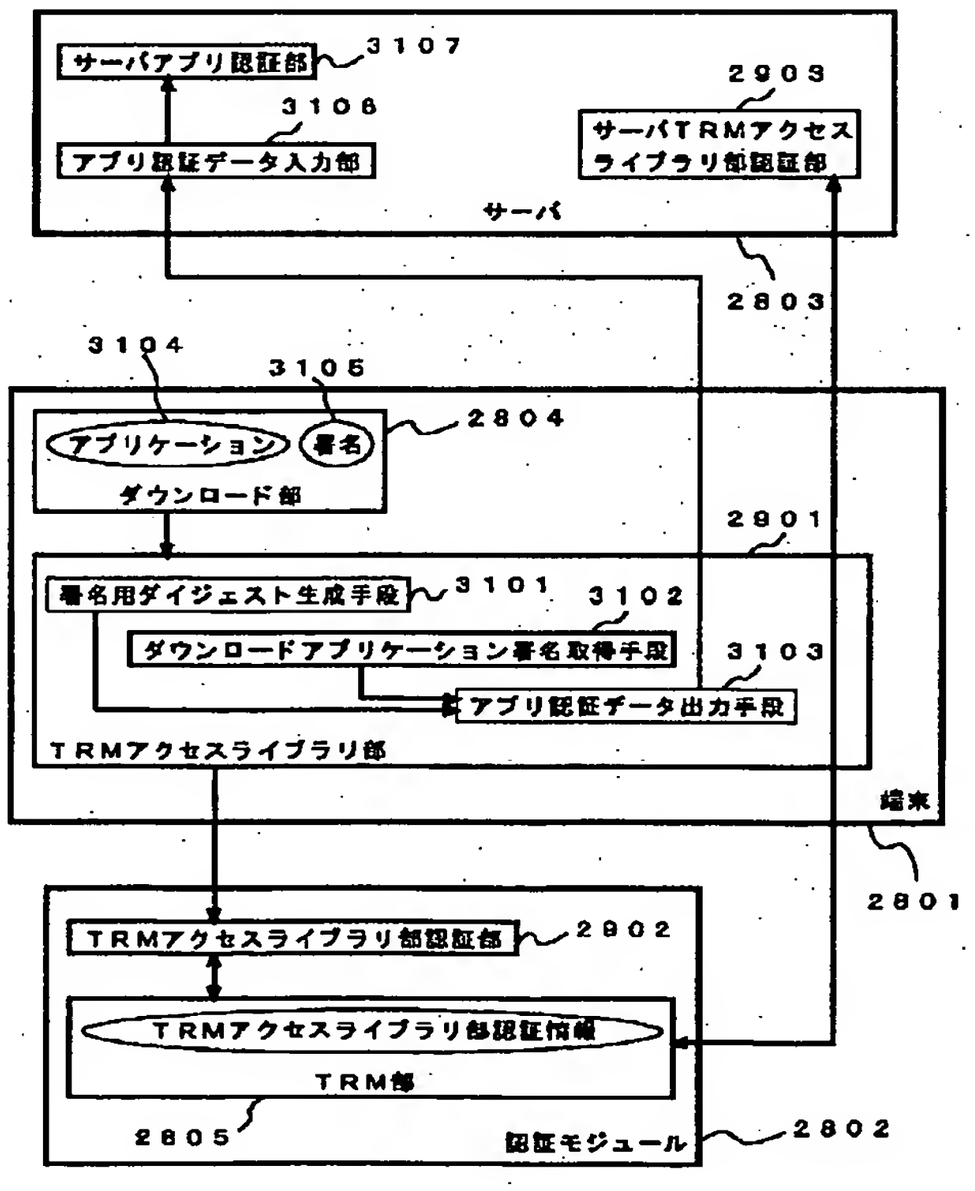
【図２９】



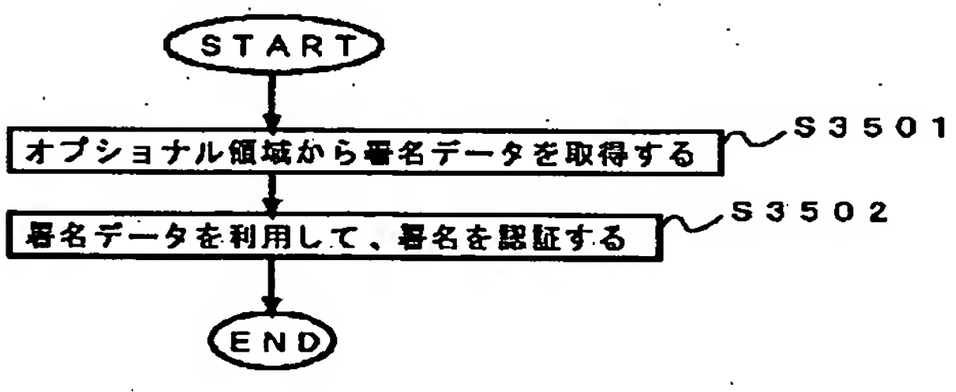
【図３０】



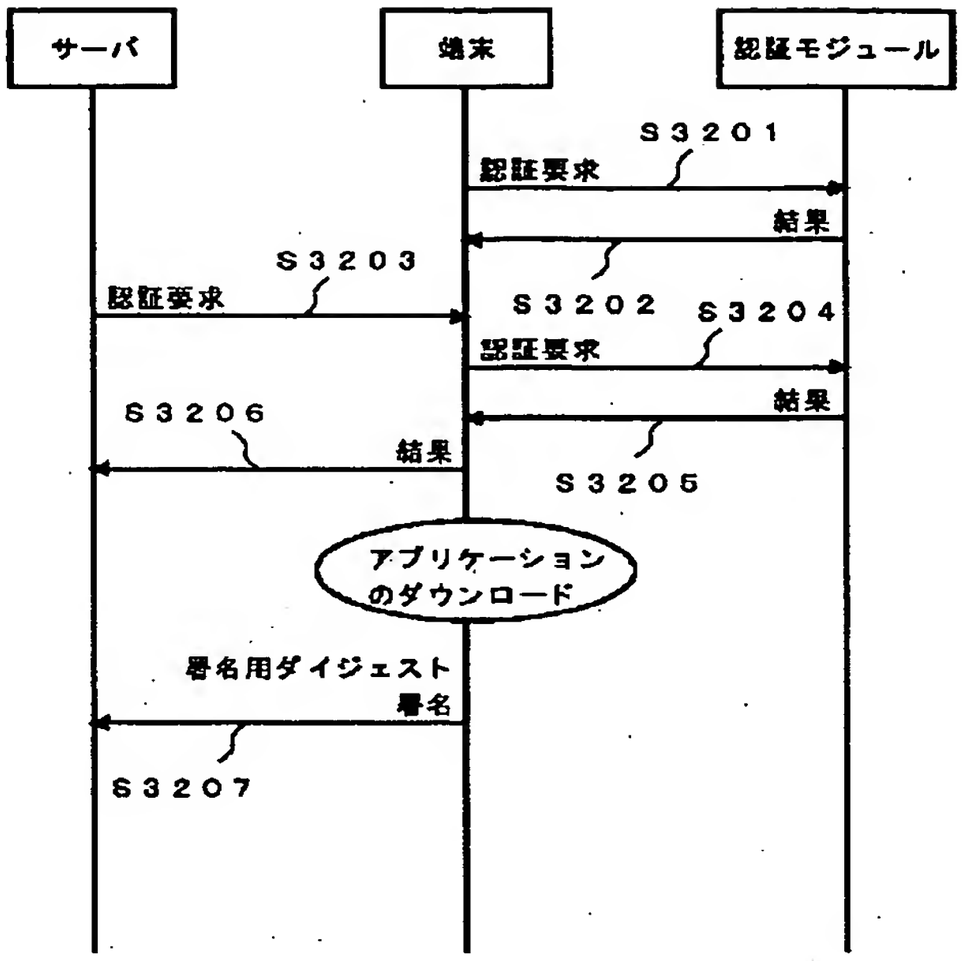
【図３１】



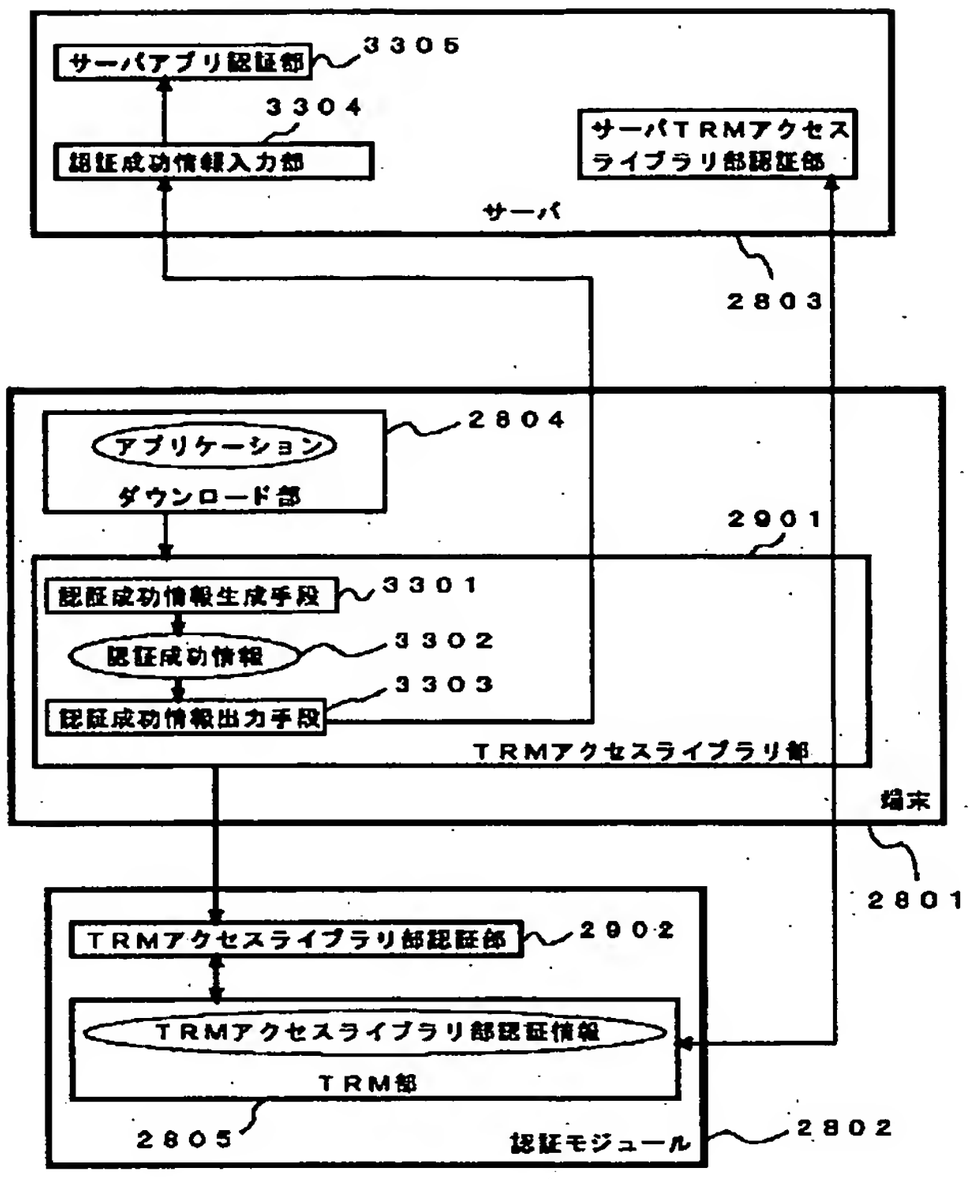
【図３５】



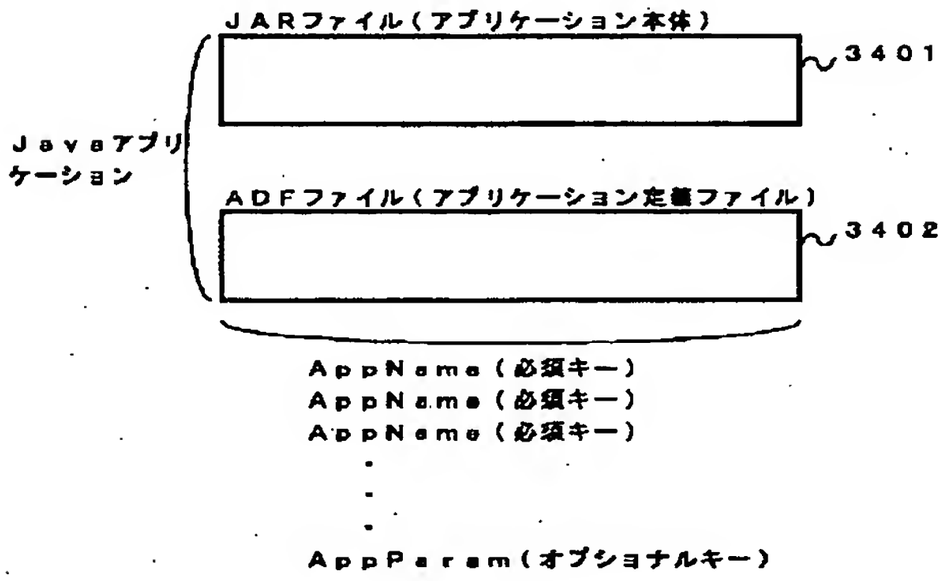
【図３２】



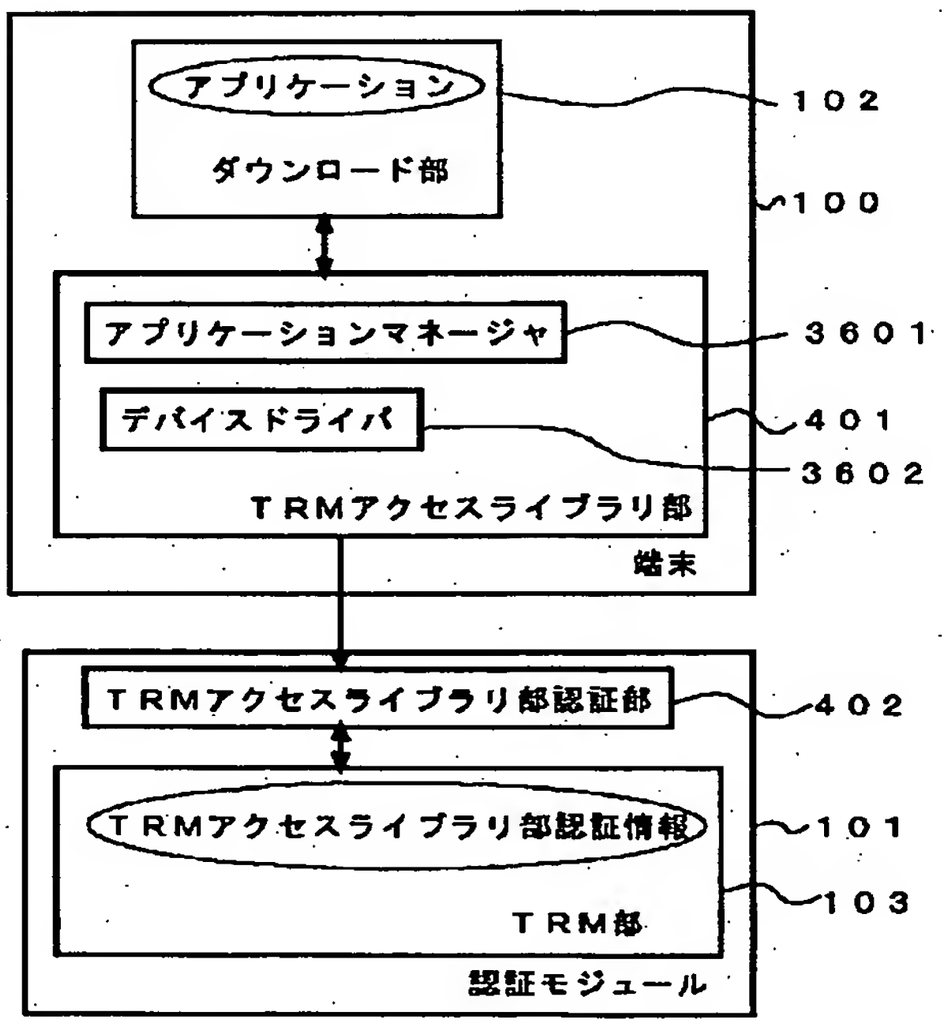
【図３３】



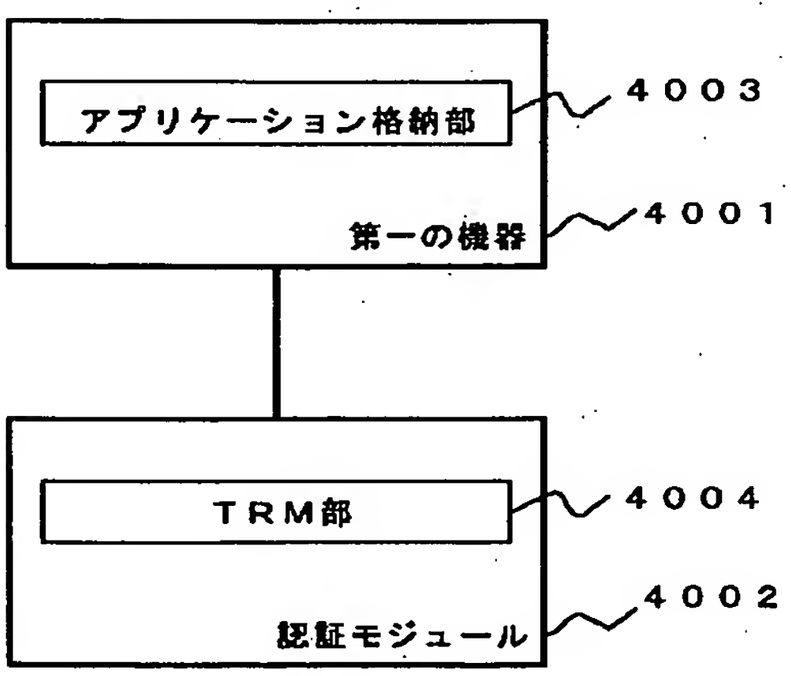
【図３４】



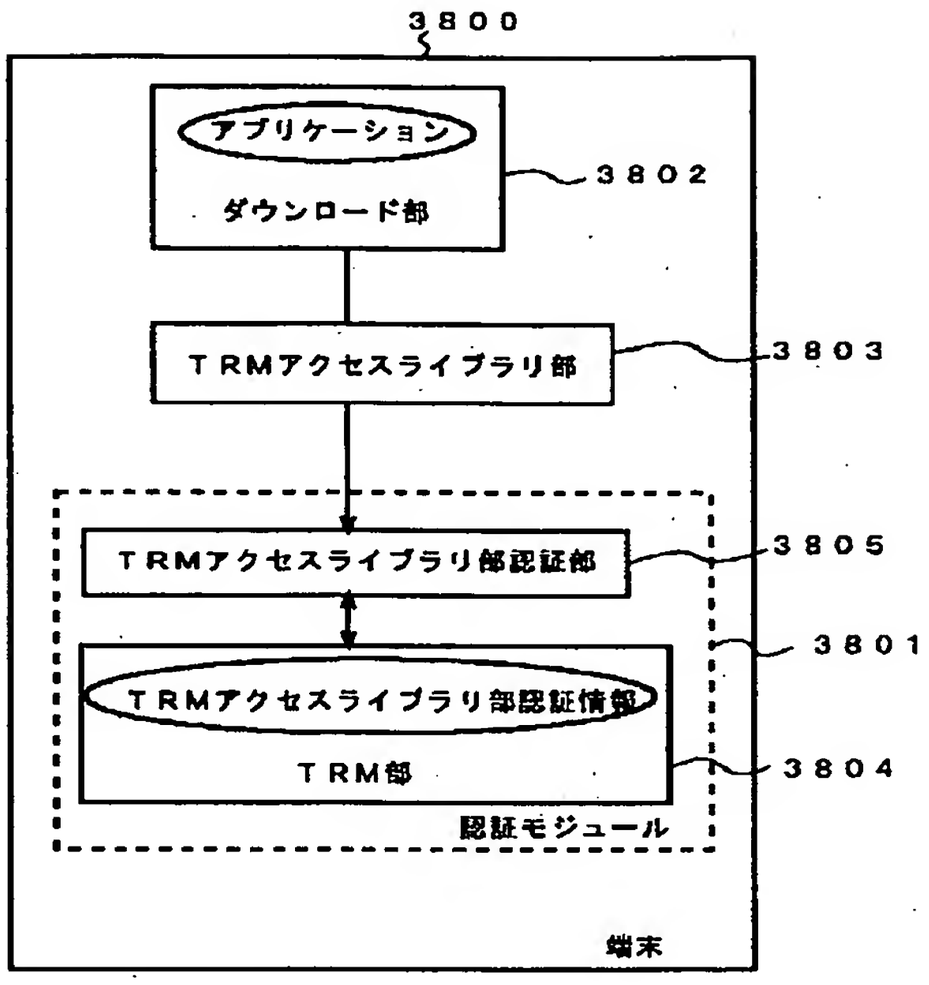
【図３６】



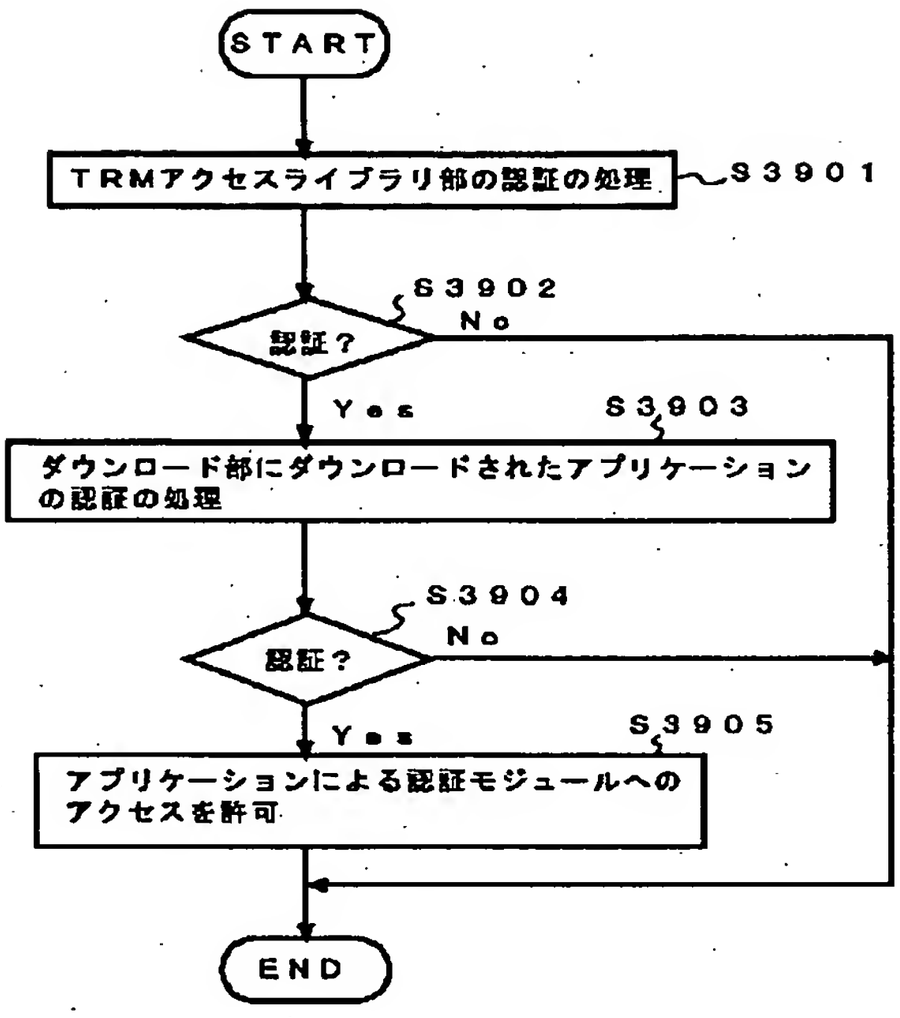
【図４０】



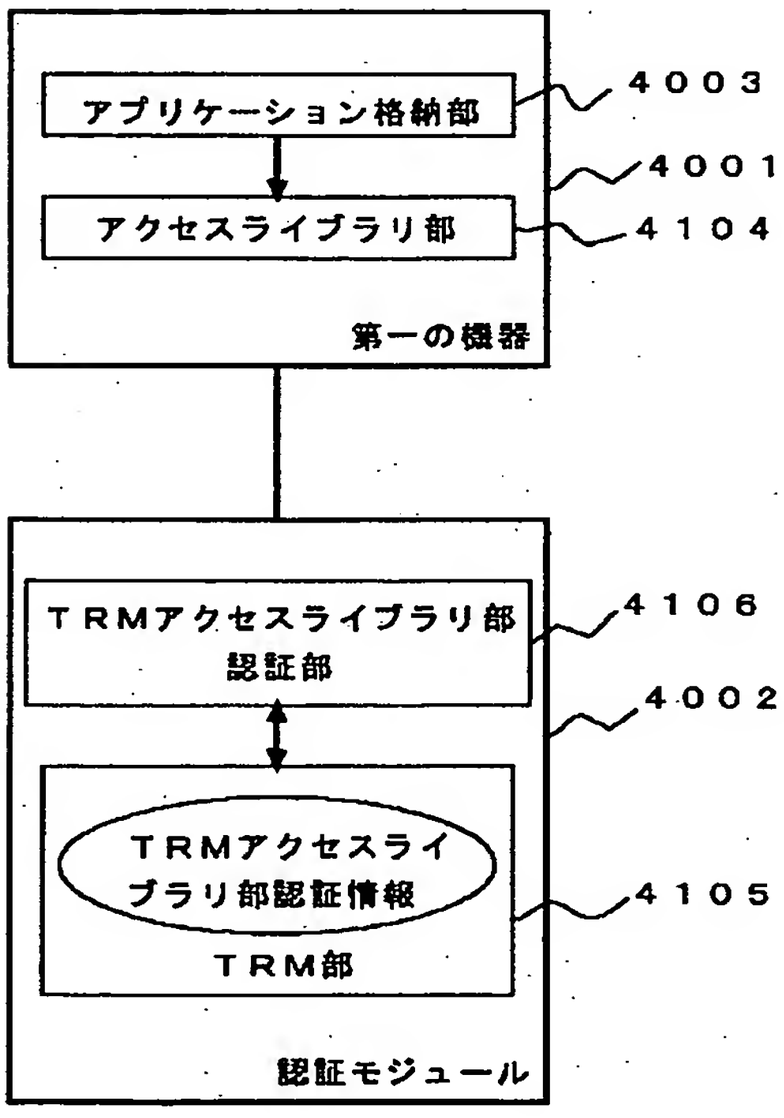
【図３８】



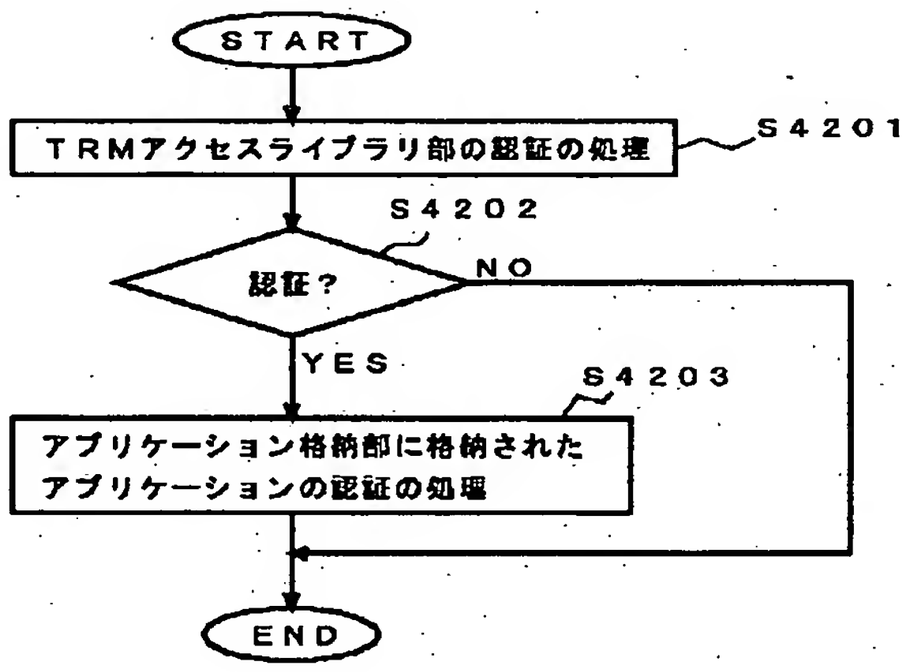
【図３９】



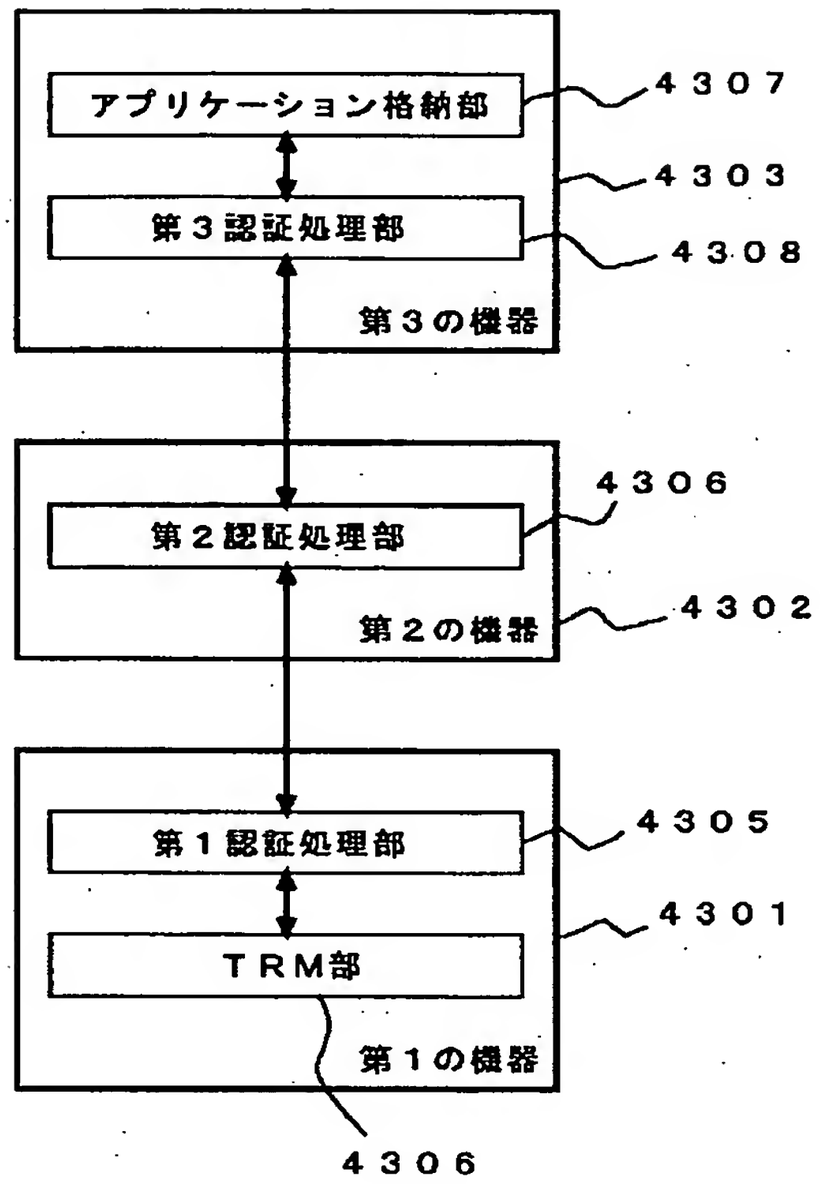
【図４１】



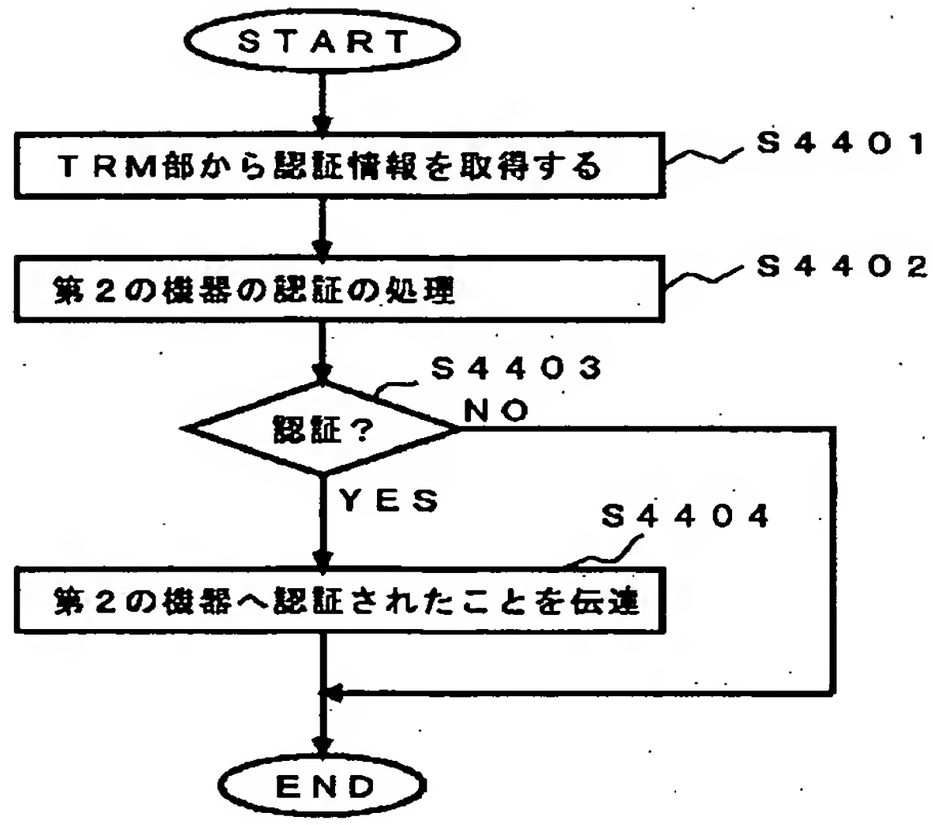
【図４２】



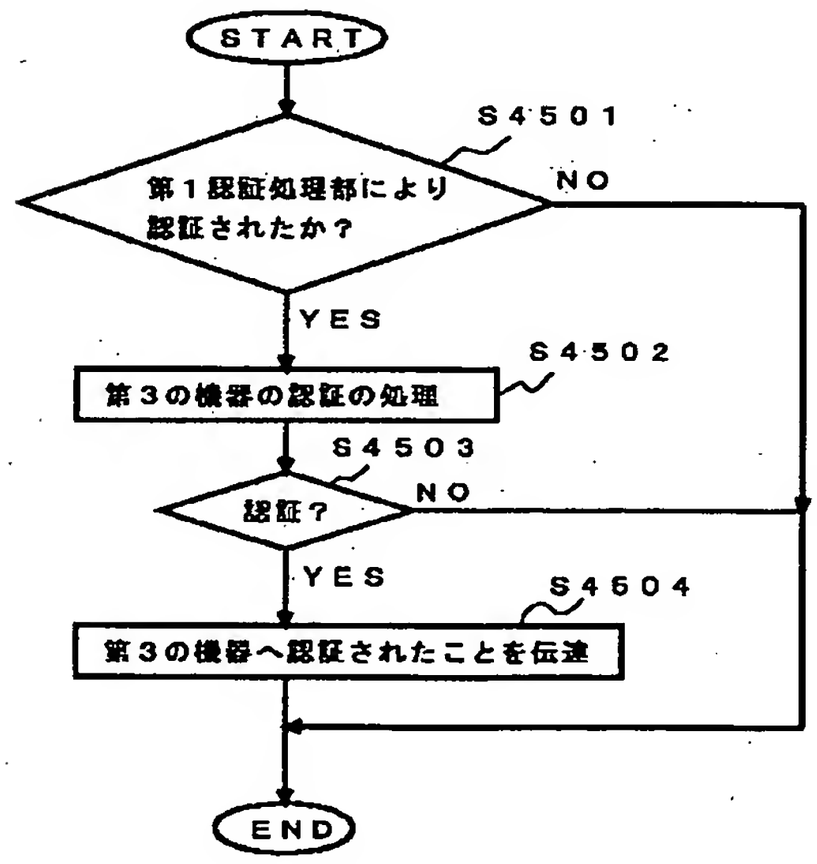
【図４３】



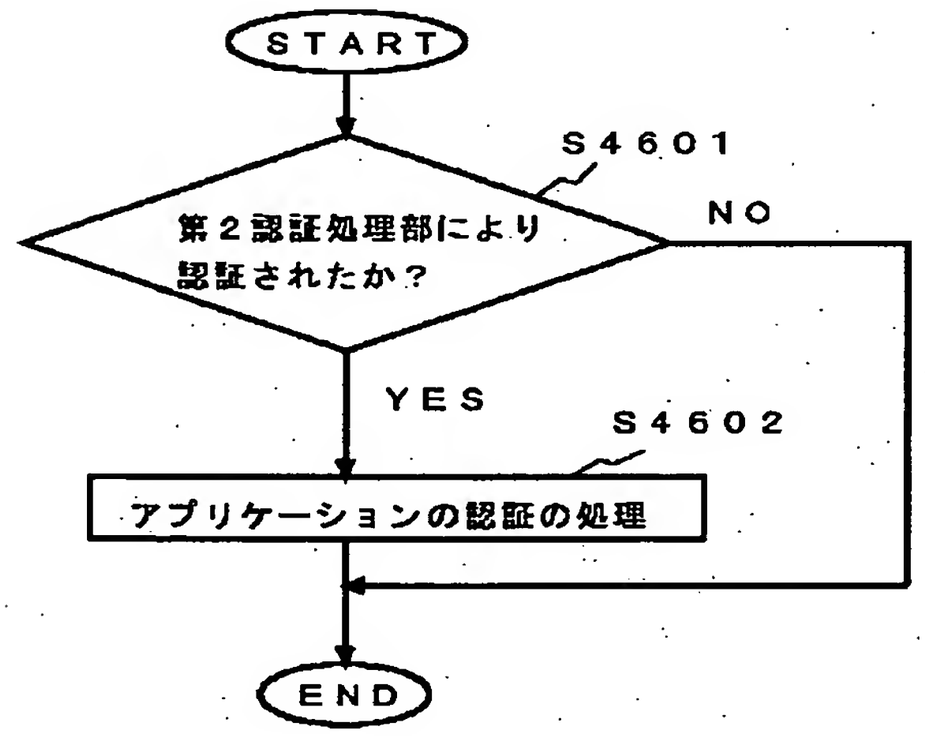
【図４４】



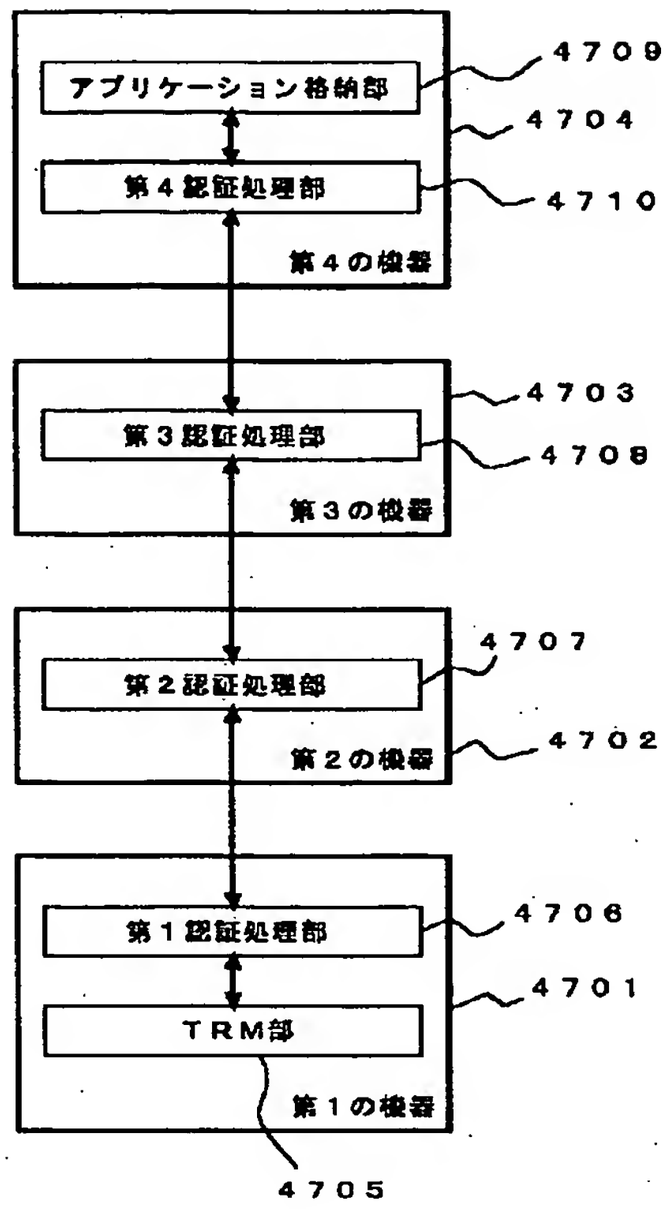
【図４５】



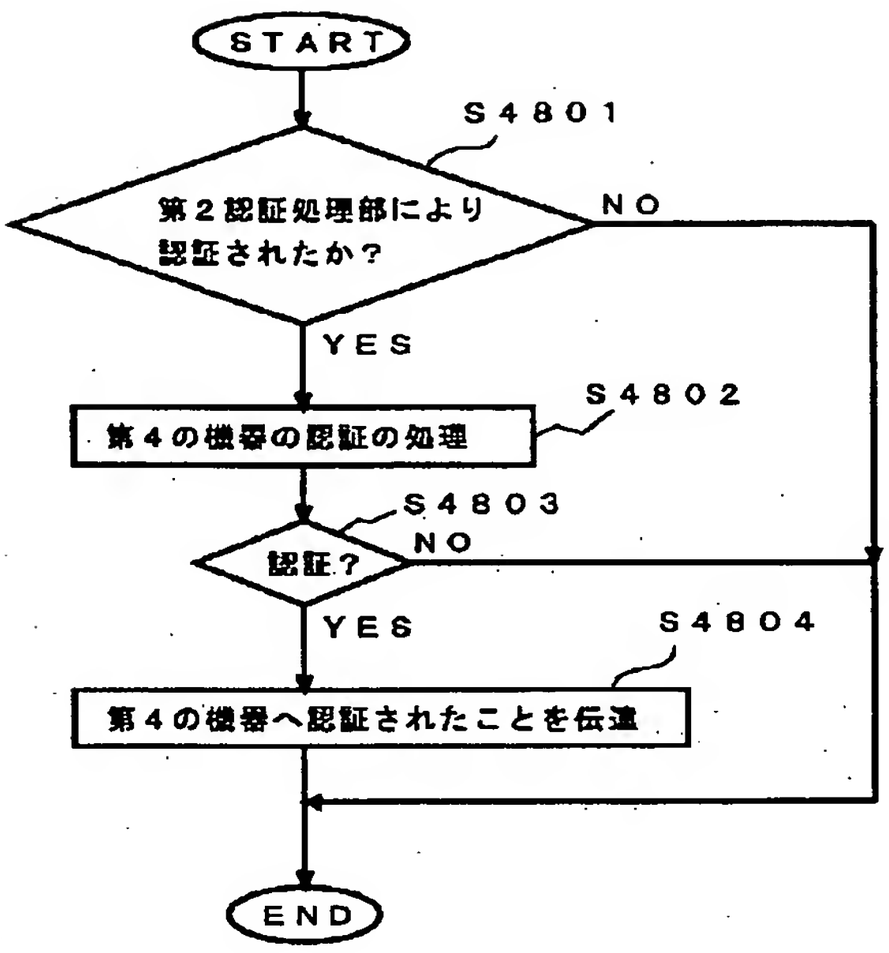
【図４６】



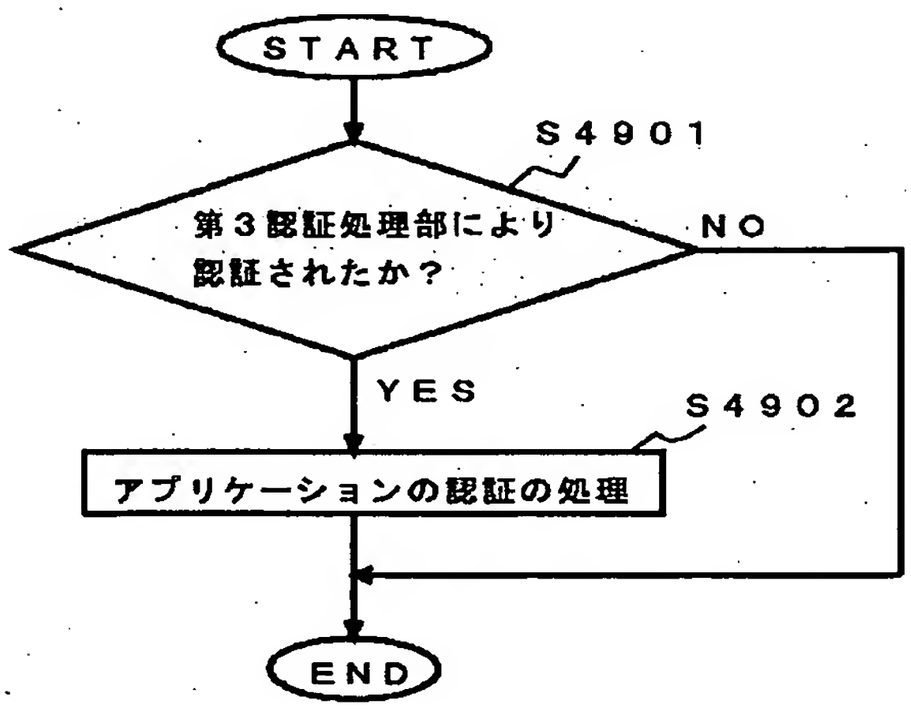
【図４７】



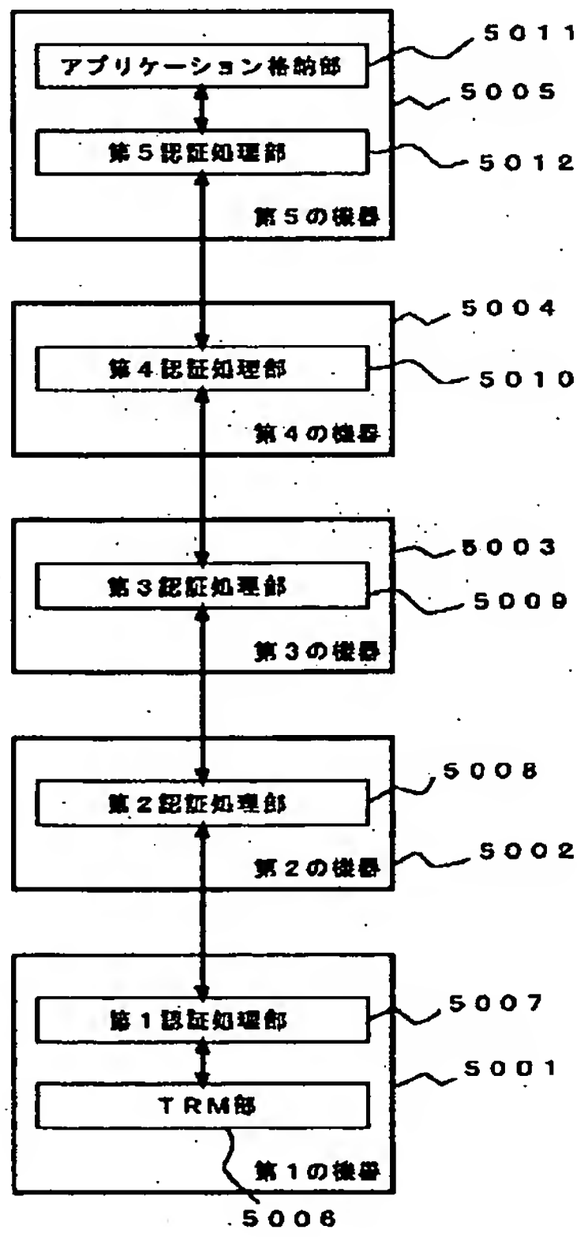
【図４８】



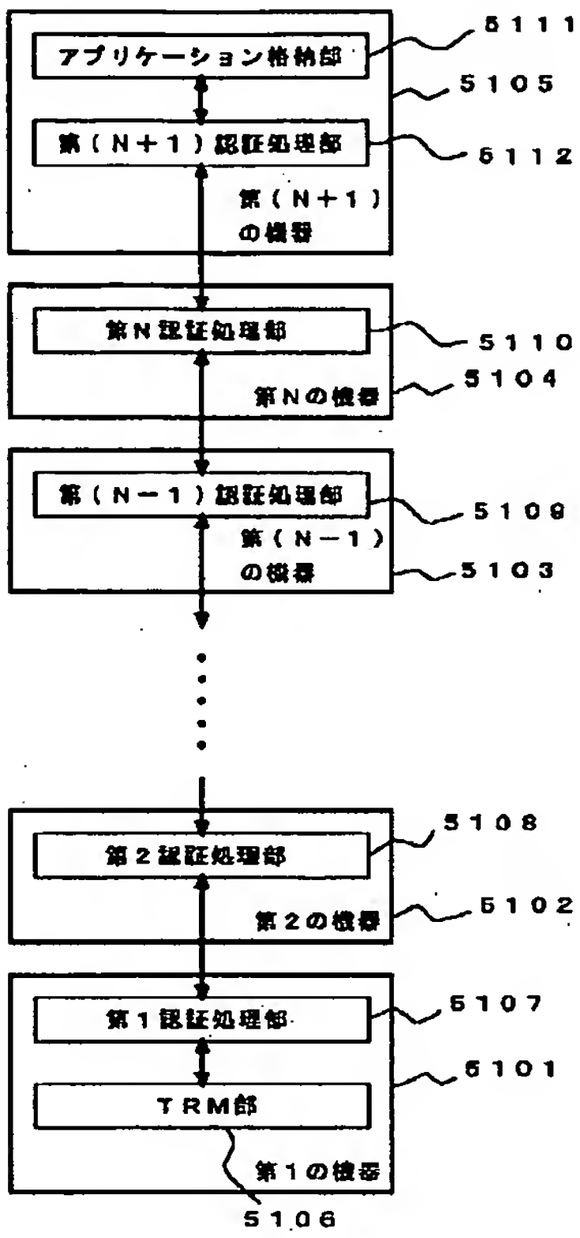
【図４９】



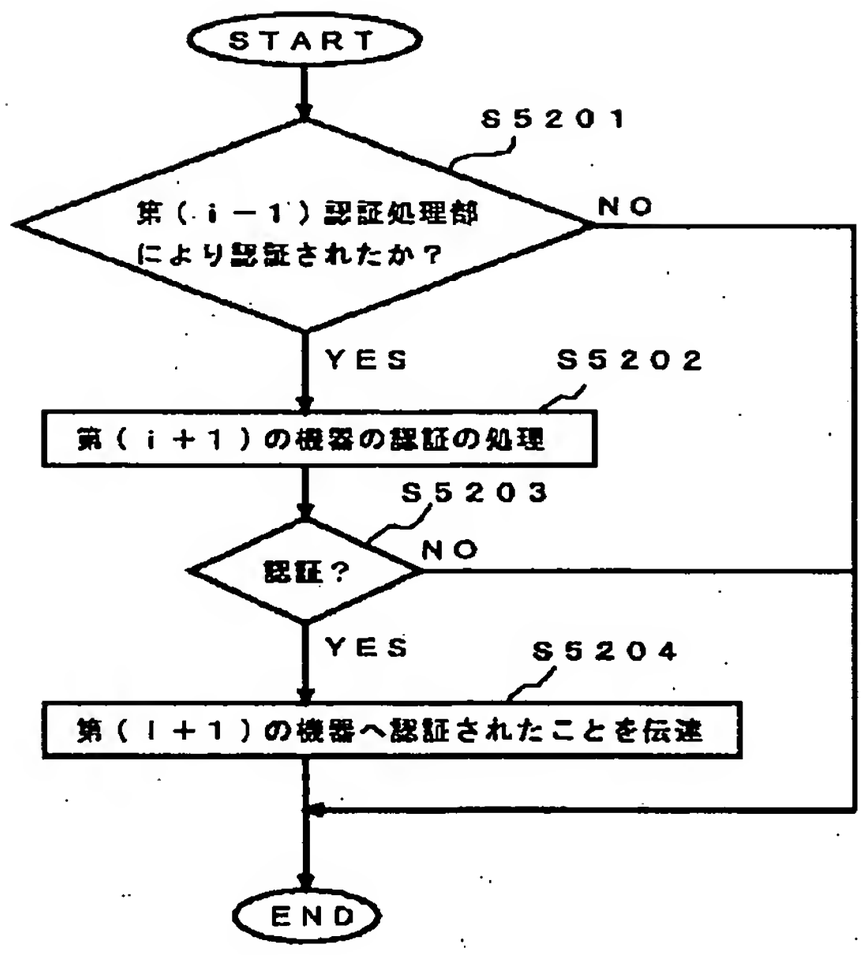
【図５０】



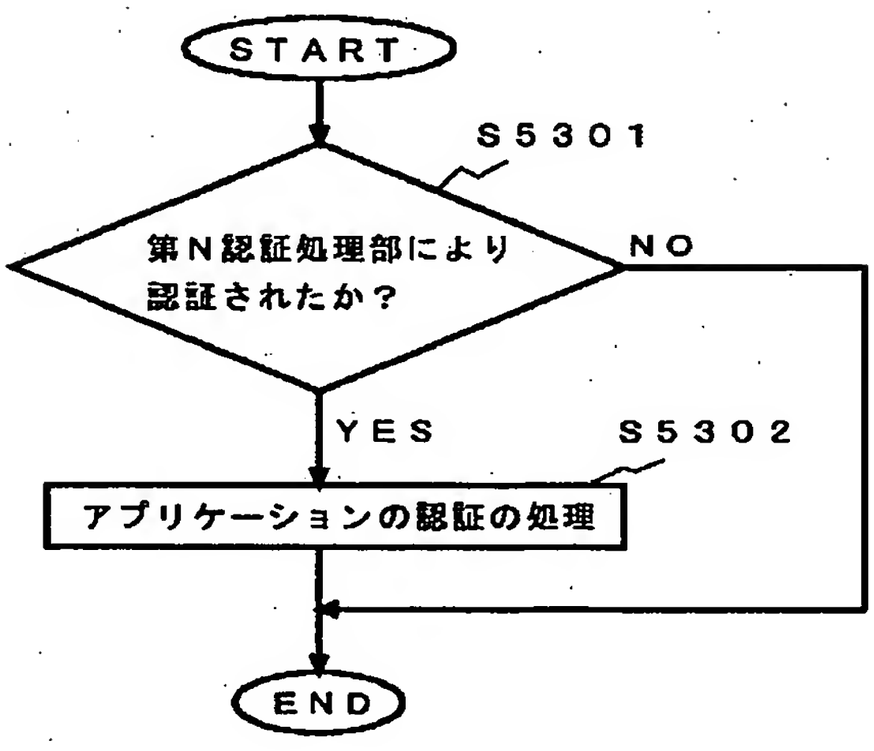
【図５１】



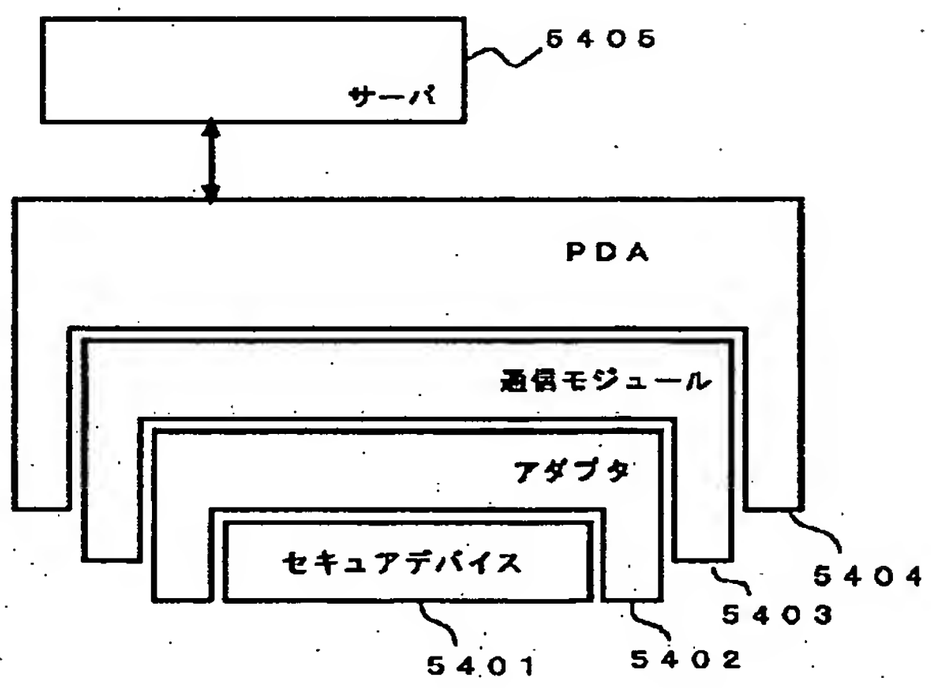
【図５２】



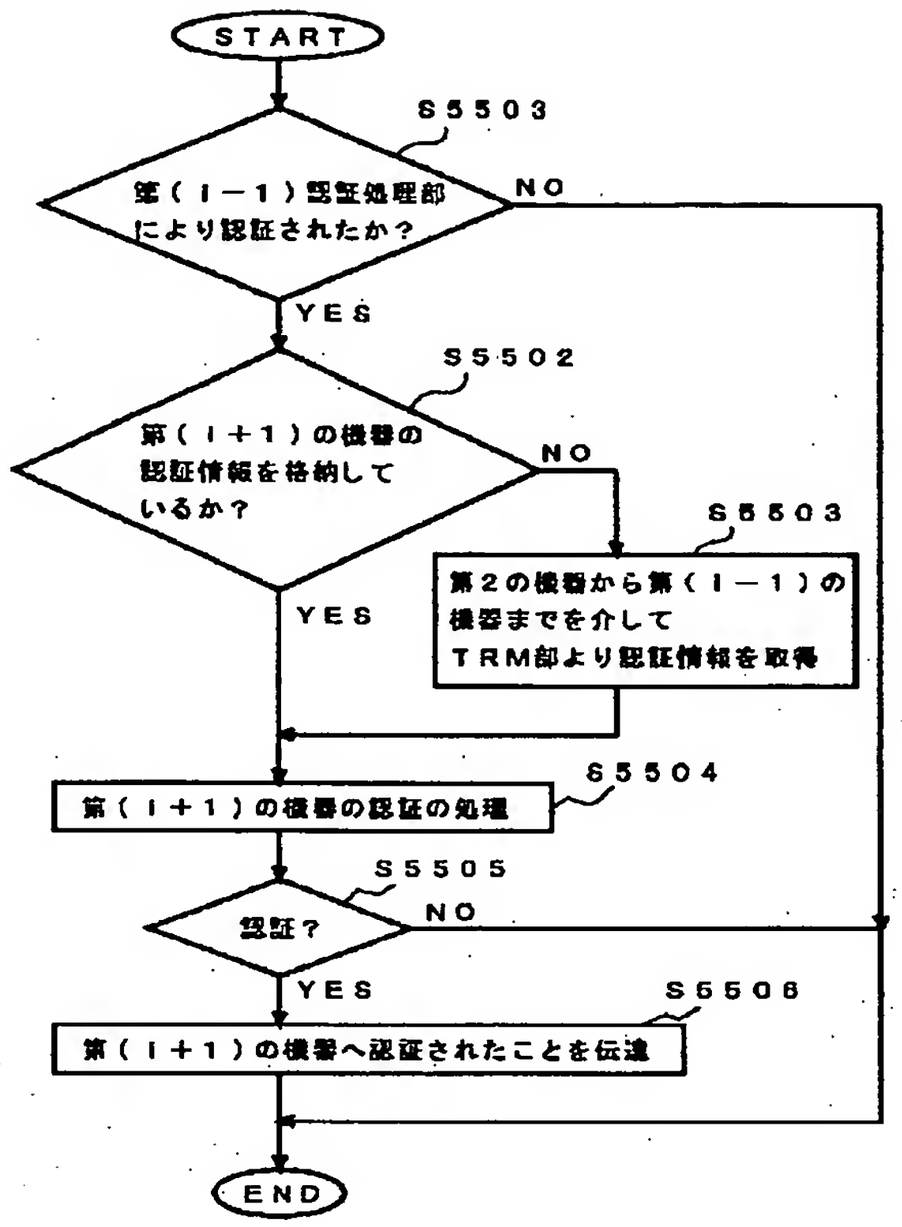
【図５３】



【図５４】



【図５５】



フロントページの続き

Ｆターム(参考) 5B035 BB09 BC00 CA11 CA29
5B058 CA23 KA01 KA04 KA32 YA20
5B076 BB06 FB02 FC07
5J104 AA08 AA09 LA01 LA05 LA06
NA12 NA35 NA38 NA40 NA41
NA42

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成17年12月22日(2005.12.22)
【公開・公表番号】特開２００３－２２３２３５
【公開日】平成15年8月8日(2003.8.8)
【出願番号】2002-321844
【国際特許分類第7版】
G06F 1/00
G06K 17/00
G06K 19/00
H04L 9/10
【ＦＩ】
G06F 9/06 660G
G06K 17/00 L
G06K 19/00 Q
H04L 9/00 621Z

【手続補正書】
【提出日】平成17年10月28日(2005.10.28)
【手続補正1】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項1】
端末と、認証モジュールと、からなるアプリケーション認証システムであって、
端末は、
アプリケーションをダウンロードするダウンロード部と、
認証モジュールに自身が認証されることを条件としてアプリケーションの認証のための処理をするＴＲＭアクセスライブラリ部と、
を有し、
認証モジュールは、
ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持するＴＲＭ部と、
ＴＲＭアクセスライブラリ部認証情報に基づいて端末のＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、
を有するアプリケーション認証システム。
【請求項2】
耐タンパ領域に情報を保持しその情報を用いて認証のための処理を行なう認証モジュールを備えた端末であって、
アプリケーションをダウンロードするダウンロード部と、
認証モジュールに自身が認証されることを条件としてアプリケーションの認証のための処理をするＴＲＭアクセスライブラリ部と、を有し、
前記認証モジュールは、
前記ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を前記耐タンパ領域に保持するＴＲＭ部と、
ＴＲＭアクセスライブラリ部認証情報に基づいて前記ＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、を有する端末。

【請求項３】
前記ダウンロード部は、改ざんのないことを認証するために用いる情報である署名が付加されたアプリケーションをダウンロードし、
前記ＴＲＭアクセスライブラリ部は、ダウンロード部にダウンロードされたアプリケーションから署名認証用ダイジェストを生成し、生成した署名認証用ダイジェストと、署名と、を含む署名認証情報を認証モジュールに出力する署名認証情報出力部をさらに有し、
前記認証モジュールは、署名認証情報出力部から出力された署名認証情報を入力する署名認証情報入力部と、
前記署名認証情報入力部から入力される署名認証用ダイジェストと、署名と、に基づいて署名の検証を行う署名認証部と、をさらに有する請求項２記載の端末。
【請求項４】
前記認証モジュールは、
前記署名認証情報入力部から入力される署名を利用して署名由来ダイジェストを生成するための署名由来ダイジェスト生成情報を取得する署名由来ダイジェスト生成情報取得部と、
前記署名認証情報入力部から入力された署名と、前記署名由来ダイジェスト生成情報取得部に保持された署名由来ダイジェスト生成情報と、を利用して署名由来ダイジェストを生成する署名由来ダイジェスト生成部とをさらに有し、
前記署名認証部は、前記署名由来ダイジェスト生成部で生成された署名由来ダイジェストと、前記署名認証情報入力部から入力された署名認証用ダイジェストと、に基づいて認証を行う請求項３に記載の端末。
【請求項５】
前記認証モジュールを認証するための認証モジュール認証部を有する請求項２から４のいずれか一に記載の端末。
【請求項６】
前記ＴＲＭアクセスライブラリ部は、認証されたアプリケーションに対して利用を認めるリソースに関する情報であるアプリケーション利用リソース情報を保持するアプリケーション利用リソース情報保持手段を有する請求項５に記載の端末。
【請求項７】
前記ＴＲＭアクセスライブラリ部は、前記認証モジュール認証部による認証がされた認証モジュールのＴＲＭ部に対してアプリケーション利用リソース情報を出力するアプリケーション利用リソース情報出力手段をさらに有し、
前記認証モジュールのＴＲＭ部は、該端末のＴＲＭアクセスライブラリ部のアプリケーション利用リソース情報出力手段から出力されたアプリケーション利用リソース情報を耐タンパ領域に書き換え可能に保持する請求項５または６に記載の端末。
【請求項８】
前記ＴＲＭアクセスライブラリ部は、アプリケーション利用リソース情報に基づいて、アプリケーションに対して、リソースの利用を認める請求項６または７記載の端末。
【請求項９】
署名が付されたアプリケーション利用リソース情報をダウンロードするアプリケーション利用リソース情報ダウンロード部をさらに有し、
前記ＴＲＭアクセスライブラリ部は、アプリケーション利用リソース情報ダウンロード部にダウンロードされたアプリケーション利用リソース情報に付された署名を検証することを特徴とする請求項６から８に記載の端末。
【請求項１０】
署名が付されたアプリケーション利用リソース情報をダウンロードするアプリケーション利用リソース情報ダウンロード部をさらに有し、
前記ＴＲＭアクセスライブラリ部は、アプリケーション利用リソース情報ダウンロード部にダウンロードされたアプリケーション利用リソース情報から署名認証用ダイジェストを生成し、

生成した署名認証用ダイジェストと、署名と、を含む署名認証情報を認証モジュールに出力するアプリケーション利用リソース情報署名認証情報出力部をさらに有し、
前記認証モジュールは、前記アプリケーション利用リソース情報署名認証情報出力部から出力された署名認証情報を入力するアプリケーション利用リソース情報署名認証情報入力部と、
前記アプリケーション利用リソース情報署名認証情報入力部から入力される署名認証用ダイジェストと、署名と、に基づいて署名の検証を行なうアプリケーション利用リソース情報署名認証部と、をさらに有する請求項６から８に記載の端末。
【請求項１１】
前記ＴＲＭアクセスライブラリ部認証情報が、該端末に固有の情報である請求項２記載の端末。
【請求項１２】
前記認証モジュールのＴＲＭ部にアクセスをする端末アプリケーションを保持する端末アプリケーション保持部をさらに有し、
前記認証モジュールのＴＲＭ部は、耐タンパ領域に、認証モジュール内にて動作する認証モジュール内アプリケーションを保持する認証モジュール内アプリケーション保持部をさらに有し、
前記認証モジュール内アプリケーションは、ＴＲＭアクセスライブラリ部認証部によるＴＲＭアクセスライブラリ部の認証の成功を条件として端末アプリケーションからのアクセスを受け入れて動作する請求項２から４のいずれか一に記載の端末。
【請求項１３】
前記認証モジュールのＴＲＭ部は、前記ＴＲＭアクセスライブラリ部認証部による前記ＴＲＭアクセスライブラリ部の認証の成功を条件として認証結果識別子を生成する認証結果識別子生成手段を有し、
認証モジュール内アプリケーションは、認証を示す認証結果識別子の存在を条件として端末アプリケーションに対して認証モジュール内アプリケーションに対するアクセスを可能とし、認証モジュール内アプリケーションは端末アプリケーションからのアクセスを受け入れる請求項１２に記載の端末。
【請求項１４】
前記認証モジュールのＴＲＭ部は、前記ＴＲＭアクセスライブラリ部によるアプリケーションの認証の成功を条件としてアプリ認証結果識別子を生成するアプリ認証結果識別子生成手段を有し、
認証モジュール内アプリケーションは、認証の成功を示すアプリ認証結果識別子の存在を条件として端末アプリケーションに対して認証モジュール内アプリケーションに対するアクセスを可能とし、認証モジュール内アプリケーションは端末アプリケーションからのアクセスを受け入れる請求項１２に記載の端末。
【請求項１５】
端末と、認証モジュールと、アプリケーションを端末にダウンロードするサーバと、からなるアプリケーション認証システムであって、
端末は、
アプリケーションをダウンロードするダウンロード部と、
認証モジュールに自身が認証されることを条件としてアプリケーションの認証のための処理をするＴＲＭアクセスライブラリ部と、を有し、
認証モジュールは、
ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持するＴＲＭ部と、
ＴＲＭアクセスライブラリ部認証情報に基づいて端末のＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、を有し、
サーバは、
端末のＴＲＭアクセスライブラリ部を介する認証モジュールのＴＲＭ部の認証が成功す

ることを条件としてＴＲＭアクセスライブラリ部の認証が成功したと判断するサーバＴＲＭアクセスライブラリ部認証部を有するアプリケーション認証システム。
【請求項１６】
認証モジュールを備えた端末に対し、アプリケーションを前記端末にダウンロードするサーバであって、
前記端末は、
アプリケーションをダウンロードするダウンロード部と、
前記認証モジュールに自身が認証されることを条件として前記アプリケーションの認証のための処理をするＴＲＭアクセスライブラリ部と、を有し、
前記認証モジュールは、
前記ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持するＴＲＭ部と、
ＴＲＭアクセスライブラリ部認証情報に基づいて前記ＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、を有し、
前記サーバは、
前記ＴＲＭアクセスライブラリ部を介する前記ＴＲＭ部の認証が成功した場合に限り、前記ＴＲＭアクセスライブラリ部の認証が成功したと判断するサーバＴＲＭアクセスライブラリ部認証部と、
前記サーバＴＲＭアクセスライブラリ部認証部により認証が成功したと判断された前記ＴＲＭアクセスライブラリ部により、前記アプリケーションから生成された署名用ダイジェストと、前記アプリケーションと共にダウンロードされた署名と、を入力するアプリ認証データ入力部と、
前記アプリ認証データ入力部に入力された署名用ダイジェストと、署名と、に基づいてアプリケーションの認証を行なうサーバアプリ認証部を有するサーバ。
【請求項１７】
認証モジュールを備えた端末に対し、アプリケーションを前記端末にダウンロードするサーバであって、
前記端末は、
アプリケーションをダウンロードするダウンロード部と、
前記認証モジュールに自身が認証されることを条件として前記アプリケーションの認証のための処理をするＴＲＭアクセスライブラリ部と、を有し、
前記認証モジュールは、
ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持するＴＲＭ部と、
ＴＲＭアクセスライブラリ部認証情報に基づいて前記ＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、を有し、
前記サーバは、
前記ＴＲＭアクセスライブラリ部を介する認証モジュールのＴＲＭ部の認証が成功した場合に限り、前記ＴＲＭアクセスライブラリ部の認証が成功したと判断するサーバＴＲＭアクセスライブラリ部認証部と、
前記サーバＴＲＭアクセスライブラリ部認証部により認証が成功したと判断された前記ＴＲＭアクセスライブラリ部により生成された前記アプリケーションの認証の成功を示す認証成功情報を入力する認証成功情報入力部と、
前記認証成功情報入力部に入力された認証成功情報に基づいてアプリケーションの認証を行なうサーバアプリ認証部と、を有するサーバ。
【請求項１８】
前記ダウンロード部は、アプリケーションが使用を許可または許可されないリソースを記述したアプリケーション利用リソース情報をダウンロードし、前記アプリケーションが前記リソースを使用する際、前記ＴＲＭアクセスライブラリ部に対してリソース使用の要求を出し、

前記ＴＲＭアクセスライブラリ部は、内部に保持している前記アプリケーション利用リソース情報を参照し、要求されたリソースが使用可能かどうかを判断し、使用可能であれば、要求されたリソースをアプリケーションに使用させる、請求項１に記載のアプリケーション認証システム。
【請求項１９】
ダウンロード部は、ダウンロードされたアプリケーションの実行時、又は／及び、アプリケーションの認証時に、サーバより使用許諾書をダウンロードする請求項１に記載のアプリケーション認証システム。
【請求項２０】
ダウンロード部は、ダウンロードされたアプリケーションの実行時、又は／及び、アプリケーションの認証時に、ダウンロードされた前記アプリケーション利用リソース情報の有効性をサーバに問い合わせる請求項１８に記載のアプリケーション認証システム。
【請求項２１】
第一の機器と、認証モジュールと、からなるアプリケーション認証システムであって、
第一の機器は、
アプリケーションを格納するアプリケーション格納部と、
認証モジュールに自身が認証されることを条件としてアプリケーションの認証のための処理をするＴＲＭアクセスライブラリ部と、を有し、
認証モジュールは、
ＴＲＭアクセスライブラリ部を認証するための情報であるＴＲＭアクセスライブラリ部認証情報を耐タンパ領域に保持するＴＲＭ部と、
ＴＲＭアクセスライブラリ部認証情報に基づいて第一の機器のＴＲＭアクセスライブラリ部を認証するＴＲＭアクセスライブラリ部認証部と、を有するアプリケーション認証システム。